	Requirement satisfied by vLEI Ecosystem Governance Framework	Requirement to be satisfied by ISO 20000 Certification	Requirement satisfied by vLEI Issuer Qualification Program	Requirement satisfied by KERI Operations
MUST' Statements EGF Primary Document				
Principles				
The vLEI Ecosystem Governance Framework MUST enable GLEIF's role to support and contribute to unique global persistent organizational identity as a public good.	X; GLEIF is acting as the Root of Trust under a sustainable business model			
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.	X; existence of vLEIs for Legal Entities			
The vLEI Ecosystem Governance Framework MUST leverage the principle of free and open access and use of the data in the Global LEI System regarding legal entities and their entity-level and relationships.	X; no fees to data users accessing vLEI information on GLEIS			
The vLEI Ecosystem Governance Framework MUST support GLEIF's intention to deliver the vLEI infrastructure using a technology agnostic approach and to use open source whenever possible.				X; KERI implemented through open source development and maintenance
The vLEI Ecosystem Governance Framework MUST support GLEIF's use of open standards.	X; use of standards in vLEIs (ISO, W3C, ToIP)			X; KERI implemented through open source development and maintenance
The vLEI Ecosystem Governance Framework MUST fulfill GLEIF's intention to make the vLEI infrastructure widely available and broadly useful as possible.	X; applicability of vLEI to digital organizational identity across use cases and domains		X; availability of Qualified vLEI Issuers on a global basis	X; KERI interoperability and portability
The vLEI Ecosystem Governance Framework MUST enable interoperability, for the digital identity data of an entity to be represented, exchanged, secured, protected, and verified interoperably using open, public, and royalty-free standards, as well as portability, the ability of identity rights holders to move or transfer a copy of their digital identity data to the agents or systems of their choice.				X; KERI interoperability and portability
The vLEI Ecosystem Governance Framework MUST empower vLEI Credential holders to secure their digital identity data at rest and in motion, to control their own identifiers and encryption keys, and to employ end-to-end encryption for all interactions and to protect the privacy of their digital identity data when applicable.				X; KERI cryptography and security features; quantum proof
The vLEI Ecosystem Governance Framework MUST ensure verifiability and authenticity by empowering vLEI Credential holders to provide verifiable proof of the authenticity of their digital identity data.	X; vLEI Credential Identity Verification Requirements		X; vLEI Credential Identity Verification Requirements	X; Credential verification process
The vLEI Ecosystem Governance Framework MUST allow vLEI Ecosystem Members to be accountable to each other for conformance to the purpose, principles, and policies of the vLEI Ecosystem Governance Framework. All vLEI Ecosystem Members MUST be responsible and be able to demonstrate compliance with any other requirements of applicable law.		X; annual certification	X; confirmation during Annual vLEI Issuer Qualification for both Qualified vLEI Issuer and GLEIF	
General Requirements				
1. All LEIs contained in vLEI Credentials MUST maintain an entity status of Active and an LEI registration status other than Lapsed, Retired, Duplicate, Annulled or Merged (will be deprecated in March 2022).	X; requirement in Credential Frameworks	X; check using GLEIF API	X; check using GLEIF API	
2. All Issuers of vLEI Credentials MUST verify that a Holder's Autonomic Identifier (AID) is controlled by the Holder.			X; mandatory check in vLEI Issuer Credential Issuance workflow	X; covered as part of the Credential issuance process with KERI
3. All Qualified vLEI Issuers (QVIs) MUST have executed a vLEI Issuer Qualification Agreement.			X; executed vLEI Issuer Qualification Agreements	
4. All QVIs MUST successfully complete Annual vLEI Issuer Qualification.			X; confirmation of Annual vLEI Issuer Qualification by GLEIF	
5. GLEIF MUST publish the vLEI Ecosystem Governance Framework on gleif.org and follow the policies in the Revisions section for all revisions of the vLEI Ecosystem Governance Framework.		X; gleif.org section for vLEI Ecosystem Governance Framework		
6. vLEI Credentials MUST be revocable following the policies specified in vLEI Ecosystem Governance Framework.		X; GLEIF revocation of Credentials service level monitoring	X; Qualified vLEI Issuer revocation of Credentials service levels	X; KERI revocation functionality
7. QVIs MUST ensure that third-parties comply with the vLEI Ecosystem Governance Frameworks when providing vLEI services to a QVI.			X; documentation provided by Qualified vLEI Issuers	
8. At a minimum, the vLEI Ecosystem Governance Framework MUST be reviewed annually.		X; GLEIF process monitoring		
9. All revisions to the Primary Document MUST be identified with a revision number that is a sequential integer.		X; compliant to Documented Information Procedure		
Revisions				
1. All revisions to Controlled Documents MUST be identified with a revision number that is a sequential integer.		X; Document approvals follow the defined Documented Information Procedure		
2. All revisions to the vLEI Ecosystem Governance Framework MUST be approved by GLEIF using its Change Management Process.		X; Document approvals follow the defined Documented Information Procedure		
Business Requirements				
3. There MUST be availability targets defined for all vLEI services included in the Appendix 5 to the vLEI Issuer Qualification Agreement - Service Level Agreement (SLA).		X; GLEIF availablility targets documented in SLA	X; Qualified vLEI Issuer availablility targets documented in SLA	
5. The QVI MUST be solely responsible for managing the revenue that is produced and costs that are incurred in the running of its vLEI operations.			X; Qualified vLEI Issuer proof of 'business' management during Annual vLEI Issuer Qualification	
6. The QVI MUST ensure that its operations regarding vLEIs are sustainably financed.			proof of 'business' management during Annual vLEI Issuer Qualification	
7. GLEIF MUST not contribute funds of any form whatsoever for QVI operations.			X; no evidence of receipt of funds by Qualified vLEI Issuers from GLEIF	
Inclusion, Equitability and Accessibility Requirements				
GLEIF MUST design the vLEI Ecosystem to be able to make vLEIs available to any Legal Entity issued a LEI in the Global LEI System.		X; Services are defined and integrated in existing Service Management System		

	Requirement satisfied by vLEI Ecosystem Governance Framework	Requirement to be satisfied by ISO 20000 Certification	Requirement satisfied by vLEI Issuer Qualification Program	Requirement satisfied by KERI Operations
MUST' Statements Information Trust				
vLEI Ecosystem Member Privacy Policies				
2. vLEI Ecosystem Members MUST comply with any governmental regulations for information security to which their activities within the vLEI Ecosystem will be subject. This includes International or trans-national governance authorities (e.g., ISO/IEC 27001 – Information Security Management, EU General Data Protection Regulation (GDPR)).	X; although GLEIF will. not be able to determine compliance by Ecosystem members other than itself and Qualified vLEI Issuers			
3. The vLEI Ecosystem Credential Governance Frameworks MUST specify the claims values to be protected by the applicable privacy policy in the jurisdiction of the Legal Entity.	X; although GLEIF will. not be able to determine compliance by Ecosystem members other than itself and Qualified vLEI Issuers			
vLEI Ecosystem Member Data Protection Policies				
1. vLEI Ecosystem Members MUST confirm that they respect and comply with data protection legislation as applicable and in force.	X; although GLEIF will. not be able to determine compliance by Ecosystem members other than itself and Qualified vLEI Issuers		X; confirmation during Annual vLEI Issuer Qualification	
2. Where no such legislation is in force, and as a material minimum standard, vLEI Ecosystem Members MUST comply with the provisions of the Swiss Federal Data Protection Act specified in the Appendix to this policy document.	X; although GLEIF will. not be able to determine compliance by Ecosystem members other than itself and Qualified vLEI Issuers		X; confirmation during Annual vLEI Issuer Qualification	
4. Qualified vLEI Issuers MUST annually review and document that the provisions of Section 5, vLEI Ecosystem Member Data Protection Policies, are implemented and enforced.			X; confirmation during Annual vLEI Issuer Qualification	
5. When a privacy breach is suspected, the involved vLEI Ecosytem Members MUST inform each other about actual or potential disclosure(s) of Personal Data and promptly take appropriate measures to address the situation and to limit the risk of such disclosure(s) from reoccurrence.	X; although GLEIF will. not be able to determine compliance by Ecosystem members other than itself and Qualified vLEI Issuers		X; confirmation during Annual vLEI Issuer Qualification	
Qualified vLEI Issuers MUST document privacy breaches in an Incident Report .			X; Incident reports filed by Qualified vLEI Issuers for all privacy breaches	
vLEI Ecosystem Member Security Policies				
1. vLEI Ecosystem Members MUST publish, review annually, maintain, and comply with IT security policies and practices sufficient to protect all services that a vLEI Ecosystem Member provides in conformance with this Ecosystem Governance Framework and meets the minimum elements of the following recommendations: https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/#gref	X; Although GLEIF will. not be able to determine compliance by Ecosystem members other than itself and Qualified vlEI Issuers	X; audit of GLEIF compliance	X; confirmation during Annual vLEI Issuer Qualification	
2. These policies MUST be mandatory for all employees of the vLEI Ecosystem Member involved with vLEI Transactions or vLEI Data. The vLEI Ecosystem Member MUST designate its Information Security Manager or another officer to provide executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.	X; Although GLEIF will. not be able to determine compliance by Ecosystem members other than itself and Qualified vlEI Issuers	X; adherence to vLEI Information Trust Policies into services and processes for which GLEIF Information Security Officer is responsible	X; adherence to vLEI Information Trust Policies into services and processes for which Qualified vLEI Issuer Information Security Officer is responsible	
3. vLEI Ecosystem Member employment verification policies and procedures MUST include, but may not be limited to, criminal background check and proof of identity validation .	X; Although GLEIF will. not be able to determine compliance by Ecosystem members other than itself and Qualified vlEI Issuers	X; inclusion of required employment verification policies and procedures into GLEIF Human Resources hiring process	X; inclusion of required employment verification policies and procedures into Qualified vLEI Issuer Human Resources hiring process	
4. Qualified vLEI Issuers MUST recertify annually that they maintain a law abiding and ethical status in the business community as evidenced in the Annual vLEI Issuer Qualification.			X; confirmation during Annual vLEI Issuer Qualification	
5. If a Qualified vLEI Issuer performs handling of vLEI Data in its own data center, the Qualified vLEI Issuer's security policies MUST also adequately address physical security and entry control according to industry best practices.			X; confirmation during Annual vLEI Issuer Qualification	
6. If a Qualified vLEI Issuer uses third-party providers in functions that involve the handling of vLEI Data, the Qualified vLEI Issuer MUST ensure that the security, privacy, and data protection policies of the third-party providers meet the requirements in this document.			X; confirmation during Annual vLEI Issuer Qualification	
7. Qualified vLEI Issuers MUST make available evidence of stated compliance with these policies and any relevant accreditations held by the Qualified vLEI Issuer during Annual vLEI Issuer Qualification, including certificates, attestations, or reports resulting from accredited third-party audits, such as ISO 27001, Statement on Standards for Attestation Engagements Service Organization Controls 2 (SSAE SOC 2), or other industry standards.			X; confirmation during Annual vLEI Issuer Qualification	
Security Incidents Policies				
1. Qualified vLEI Issuers MUST maintain and follow documented incident response procedures and guidelines for computer security incident handling and will comply with data breach notification terms of the vLEI Issuer Qualification Agreement. ITIL (Information Technology Infrastructure Library) Incident Management is followed by GLEIF and is certified as part of GLEIF's ISO 20000 certification.			X; confirmation during Annual vLEI Issuer Qualification	
2. Qualified vLEI Issuers MUST define and execute an appropriate response plan to investigate suspected unauthorized access to vLEI Data. This plan MUST include procedures and forms that GLEIF and the Qualified vLEI Issuers use responsively to communicate security events and their disposition.			X; appropriate response plan provided to GLEIF during vLEI Issuer Qualification and confirmed during Annual vLEI Issuer Qualification; existence of forms communicating security events and their disposition	
Availability Policies				
1. GLEIF and Qualified vLEI Issuers MUST maintain defined availability targets as part of the vLEI Ecosystem Governance Framework.		X; defined GLEIF availability targets in SLA	X; confirmation during Annual vLEI Issuer Qualification	
2. GLEIF and Qualified vLEI Issuers MUST maintain records to evidence the availability of their services.		X; audit of GLEIF compliance	X; confirmation during Annual vLEI Issuer Qualification	
Developer Security Policies				
1. GLEIF MUST provide technical changes/upgrades to the GLEIF-supplied vLEI software to Qualified vLEI Issuers.		X; audit of GLEIF compliance		
2. Qualified vLEI Issuers MUST successfully install, test and implement the GLEIF-supplied vLEI software within stated timeframes.			X; software working by stated timeframes	

MUST' Statements Technical Requirements Part 1: KERI Infrastructure	Requirement satisfied by vLEI Ecosystem Governance Framework	Requirement to be satisfied by ISO 20000 Certification	Requirement satisfied by vLEI Issuer Qualification Program	Requirement satisfied by KERI Operations
Specification Version Upgrades				
1. Previous versions explicitly cited by policies in this document MUST be supported for a period 18 mo	X			
2. 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.	X			
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.			X; assessment and demonstration of compliance	
Endorser (Backer) Management				
Witness Pool:				
1. MUST use KAACE sufficient majority threshold on a minimum pool of 5 Witnesses.			X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
3. MUST publish Witnesses to at least one ecosystem discovery mechanism:			X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
a. Well-Known URI IETF RFC-8615 on a web site(s)associated with entity. The value of the /.well-known/oobi resource is a KERI OOBI (out-of-band-introduction) to witness or witnesses			X; assessment and demonstration of compliance	
b. Publish KERI OOBIs for witnesses on web site(s) discoverable by search engines.				
c. KERI Distributed Hash Table (DHT)			X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
d. DID method resolvers			X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
e. Ledgers			X; assessment and demonstration of compliance	
Registrar (Ledger)				
1. MUST use a GLEIF Approved DID Method (one for each authorized ledger): a. Security guarantees are based on the particular ledger b. A DID method MUST be approved down to the ledger-specific level.			X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
Hybrid (Witness Pool and Ledger Registrar):			X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
1. MUST use only one type for any KEL.				X; covered by KERI Key Management Architecture
Key-pair creation and storage infrastructure				
1. Strength				
All key-pairs MUST be generated using a cryptographic algorithm with at least 128 bits of cryptographic strength. This includes using a source of entropy of at least 128 bits of cryptographic strength for the salt or seed used to generate the private key of the key pair.				X; covered by KERI Key Management Architecture
2. Autonomic Identifiers (AIDs)				
1. Both Verifiable Credential (VC) Issuer and Issuee AIDs MUST be transferable.				X; covered by KERI Key Management Architecture
Key Pre-Rotation for Transferable AIDs				
1. The next or pre-rotated set of keys MUST be protected with the highest level of protection. This level of protection should be commensurate with the value of the assets these keys are protecting.			X; confirmation during Annual vLEI Issuer Qualification	
Non-delegated pre-rotated keys are at the root level of a delegation hierarchy and MUST have the very highest level of protection. There is no recovery mechanism within KERI to regain control over a non-delegated AID once its pre-rotated keys have been captured. The only recourse is to abandon the AID and stand up a new AID and reestablish the reputation and associations of the new AID. This re-establishment process is ecosystem dependent and is not part of KERI.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
Signature Verification Infrastructure				
1. Best practices for code delivery and library usage MUST be observed for signature verification infrastructure.			X; confirmation during Annual vLEI Issuer Qualification	
GLEIF Root AID Inception Event				
1. GLEIF MUST hold a recorded GLEIF Root AID Genesis Event with at least [number] of Notaries as witnesses			X; assessment and demonstration of GLEIF compliance	
2. The KEL for the GLEIF Root AID Genesis Event:				
a. MUST be stored on the following GLEIF servers protected by extended validation HTTPS certificates:			X; assessment and demonstration of GLEIF compliance	
i. [need list of GLEIF HTTPS servers]				
b. MUST be stored at the following HTTPS URLs of affiliated organizations:			X; assessment and demonstration of GLEIF compliance	
i. [need list of HTTPS URLs that will be used at each affiliated organization, e.g., LEI Issuers, Qualified vLEI Issuers, ROC members, etc.]				
c. MUST be stored as a file on a public GLEIF GitHub repository.			X; assessment and demonstration of GLEIF compliance	
d. MUST be shared on the following social media:			X; assessment and demonstration of GLEIF compliance	
i. [need list of social media, e.g., LinkedIn, Twitter, other long-lived secure public archives]				
GLEIF Root AID				
1. Non-delegated pre-rotated keys are at the root level of the delegation hierarchy and MUST have the very highest level of protection				
2. MUST be a threshold multisig with weighting requirements that have been determined by GLEIF.	X			X; covered by KERI Key Management Architecture
3. Key Pair Creation and Storage Infrastructure MUST be within a TEE.				X; covered by KERI Key Management Architecture
4. Each key-pair in a thresholded multi-sig MUST use a non-co-located TEE.				X; covered by KERI Key Management Architecture
GLEIF Root Witness Pool				
1. The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAACE.				X; covered by KERI Key Management Architecture
2. The number of Witnesses on any single web host provider MUST be less than the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)				X; covered by KERI Key Management Architecture
3. The number of Witnesses on any single continent MUST be less than the sufficient threshold as per KAACE.				X; covered by KERI Key Management Architecture
4. The number of Witnesses in any single political jurisdiction MUST be less than the sufficient threshold as per KAACE.				X; covered by KERI Key Management Architecture

GLEIF Root Witness Signing Key Pair key store MAY reside on the Witness Service host but MUST use dedicated user only permissions on the key store directory and its contents. The secrets in the key store MUST be encrypted with the key loaded dynamically whenever the Witness service is started. The key store MUST reside on a different device or host from that of the Witness service.				X; covered by KERI Key Management Architecture
GLEIF External Delegate AID				
They are the same as GLEIF Internal Delegate AID except:				
1. GLEIF MUST set the Do Not Delegate configuration property on Delegated vLEI Issuer AIDs.				X; covered by KERI Key Management Architecture
GLEIF Watcher Network				Management
2. Larger pool sizes MUST use KAACE sufficient majority thresholds.				X; covered by KERI Key Management Architecture
3. The GLEIF Watcher Signing Key Pair key store MAY reside on the Watcher Service host but MUST use dedicated user only permissions on the key store directory and its contents.				X; covered by KERI Key Management Architecture
5. When used, the encryption key store MUST reside on a different device or host from that of the Watcher service.				X; covered by KERI Key Management Architecture
GLEIF Key Management Policies				
1. The specific holders of cryptographic keys MUST be kept confidential and shall be determined by GLEIF internal policy.			X; assessment and demonstration of GLEIF compliance	
3. Signing keys MUST be rotated whenever there is a likelihood of key compromise.				X; covered by KERI Key Management Architecture
4. The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.			X; assessment and demonstration of GLEIF compliance	
6. GLEIF policies for approving rotation of the issuing keys for the GLEIF-Delegated issuing identifier:				X; covered by KERI Key Management Architecture
a. MUST use an OOB (out-of-band) MFA (multi-factor authorization) mechanism to approve Delegated AID rotation.			X; assessment and demonstration of GLEIF compliance	
Qualfied vLEI Issuer KERI Profile				
Qualified vLEI Issuers Delegated ID				
1. For added security, Qualified vLEI Issuers:				
a. MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
b. MUST use at least a 2 or 3 thresholded multi-sig scheme.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
3. Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
Qualified vLEI Issuer Endorser Support: Witness Pool or Ledger Registrar				
1. An Endorser MUST use either a Witness Pool or a Ledger Registrar for Endorsement			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
Qualified vLEI Issuer Witness Pool				
1. The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAACE.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
2. The Witness Signing Key Pair key store MAY reside on the Witness Service host but MUST use dedicated user only permissions on the key store directory and its contents.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
4. The encryption key store MUST reside on a different device or host from that of the Witness service.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
Qualified vLEI Issuer Ledger Registrar				
1. Registrar Signing Key Pair key store MAY reside on the Registrar Service host but MUST use dedicated user only permissions on the key store directory and its contents.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
3. The encryption key store MUST reside on a different device or host from that of the Registrar service.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
Qualified vLEI Issuer Watchers				
2. Larger pool sizes MUST use KAACE sufficient majority thresholds.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
3. Watcher Signing Key Pair key store MAY reside on the Watcher Service host but MUST use dedicated user only permissions on the key store directory and its contents.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
5. When used, the encryption key store MUST reside on a different device or host from that of the Witness service.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
Qualified vLEI Issuer Key Management				
1. The specific holders of cryptographic keys MUST be kept confidential and shall be determined by Qualified vLEI Issuer internal policy.			X; confirmation during Annual vLEI Issuer Qualification	
3. Signing keys MUST be rotated whenever there is a likelihood of key compromise.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
4. The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.			X; confirmation during Annual vLEI Issuer Qualification	
Qualified vLEI Issuer Delegation				
1. The Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to True.			X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
Qualified vLEI Issuer Key Compromise Monitoring				
1. MUST monitor their public VDR for their vLEI or VC issuance and revocation registry for erroneous or malicious issuances and revocations (primarily issuances) in order to in-form their key management process that a key recovery may be required.			X; confirmation during Annual vLEI Issuer Qualification	
Qualified vLEI Issuer Key Compromise Recovery				
1. In any case of key compromise, a Qualified vLEI Issuer MUST:				
a. Report to GLEIF all key compromise recovery operations within 24 hours of gaining knowledge of the key compromise.			X; confirmation during Annual vLEI Issuer Qualification	
b. Investigate as expeditiously as possible at its own expense the source of the key compromise and make a full report of the investigation to GLEIF.			X; confirmation during Annual vLEI Issuer Qualification	
c. Make a recovery rotation event that forks their KEL and submit the recovering rotation event and signatures to GLEIF in order that GLEIF may anchor a confirmation seal in its KEL.			X; confirmation during Annual vLEI Issuer Qualification	
d. Send a key recovery event explanation to GLEIF for publication in GLEIF's public registry of Qualified vLEI Issuer recovery events.			X; confirmation during Annual vLEI Issuer Qualification	
vLEI Issuance and Revocation Policies				
1. Qualified vLEI Issuers MUST monitor their public VDR for their vLEI or VC issuance and revocation registry for erroneous or malicious issuances and revocations (primarily issuances) in order to in-form their key management process that a key recovery may be required.			X; confirmation during Annual vLEI Issuer Qualification	
Challenge Message				X; covered by KERI operations
1. The Challenge Message MUST include a cryptographic nonce generated in real time.				X; covered by KERI operations

3.	The Challenge Response Message MUST be Fully Signed by the Responder.				X; covered by KERI Key Management Architecture
4.	The Challenger MUST verify that:				
	a. The Fully Signed Response contains the same cryptographic nonce as the Challenge Message.				X; covered by KERI Key Management Architecture
	b. The signatures of the Responders were generated by the private keys that control the Responder's AID.				X; covered by KERI Key Management Architecture

"MUST' statements Technical Requirements Part 2: vLEI Credentials	Requirement satisfied by vLEI Ecosystem Governance Framework	Requirement to be satisfied by ISO 20000 Certification	Requirement satisfied by vLEI Issuer Qualification Program
Specification Version Upgrades			
Previous versions explicitly cited by policies in this document MUST be supported for a period 18 months .	X		
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.	X		
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 immutablity).			
The following ACDC sections MUST include a SAID - Attribute (data payload) section, Schema section and Rules section.			
7. All source links MUST include the SAID of the referenced ACDC.			
8. ACDCs have three primary forms that MUST be supported separately by Issuers, Holders and Verifiers usingthe following rules:	X		
Form 1 – the Fully-expanded Form in which the schema, attributes and rules are fully expanded and embedded.			
Form 2 – the Fully-compressed Form in which only the SAID of each major section is included.			
Form 3 – Schema-compressed Form so the only the SAID of the schema section is included.			
9. Issuers MUST support the issuance of vLEI Credentials in any or all three forms.	X		X
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.	X		X
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 immutablity).			
3. Each vLEI Credential MUST be in compliance with its specific vLEI Credential Govenance Framework.	X		
3.1. Each vLEI Credential MUST be chained to its source(s), if any, as required by the applicable vLEI Credential Govenance Framework in accordance with the ACDC specification.			
Composable Event Streaming Representation (CESR)			
1. The Proof Format for vLEI Credentials MUST comply with the CESR Proof Format specificiation.			
2. Each vLEI Credential Issuer MUST maintain a highly-available issuance and registration registry in compliance with the Public Transaction Event Log (PTEL) Specification.			
3. vLEI Credential Issuers MUST comply with the Issuance Exchange Protocol Specification for ACDC and KERI.			
Credential Registry and Revocation Registry Requirements			
1. Each vLEI Credential Issuer MUST maintain a highly-available issuance and registration registry in compliance with the Public Transaction Event Log (PTEL) Specification.			
Exchange Protocols			
1. vLEI Credential Issuers MUST comply with the Issuance Exchange Protocol Specification for ACDC and KERI.			

	Requirement satisfied by vLEI Ecosystem Governance Framework	Requirement to be satisfied by ISO 20000 Certification	Requirement satisfied by vLEI Issuer Qualification Program	Requirement satisfied by KERI Operations
MUST' Statements GLEIF Identifiers (GLEIF Root AID, GLEIF Internal and External Delegated AIDs)				
5. AID Generation				
1. An AID conformant with this Governance Framework MUST be created from two sets of asymmetric signing key pairs generated from a cryptographically-secure pseudo-random number generator (CSPRNG) or a true random number generator with at least 128 bits of cryptographic strength.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
2. The AID MUST then be derived from a cryptographic digest of a serialization of the public keys of the first set of key pairs and a cryptographic digest of second set of key pairs, as well as any other identifiers and configuration parameters associated with the supporting infrastructure for the Root Identifier as specified in the Technical Requirements Part 1 KERI Infrastructure.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
3. The cryptographic digest MUST have at least 128 bits of cryptographic strength.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
6. AID Controllers				
1. All Controllers MUST establish their own Private Key Store.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
2. All Controllers MUST keep their private keys secret.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
3. A given Controller MUST control one and only one key pair from each set of keys.	X; requirement in Identifier Governance Framework			
4. The KERI protocol MUST be used to transfer control authority from one set of keys to another.	X; requirement in Identifier Governance Framework			X; covered as part of the transfer control process with KERI
5. Continuity and Survivorship				
a. GLEIF MUST have a Continuity Policy for the survival of control authority of all Controllers for the GLEIF Root AID and its Delegated AIDs, including Escrow Controllers.	X; requirement in Identifier Governance Framework			
7. GLEIF AID Genesis				
1. GLEIF MUST establish a list of initial GLEIF Controllers that specifies:				
a. The legal identity of each Controller.	X; requirement in Identifier Governance Framework			
b. Which Controllers shall control the GLEIF Root AID, the GLEIF Internal AID and the GLEIF External AID	X; requirement in Identifier Governance Framework			
c. A set of policies MUST be put in place that ensure fault-tolerance with respect to common mode failures of the multi-sig signing authority of the set of GLEIF Controllers, e.g., a Designated Survivor policy and/or restrictions on joint travel and in-person attendance of meetings).	X; requirement in Identifier Governance Framework			
2. GLEIF MUST establish a real-time Out-of-Band Interaction (OOBI) session in which all initial GLEIF Controllers are present. An example is a continuous webmeeting attended by all parties on both audio and video.	X; requirement in Identifier Governance Framework			
a. This session MUST be recorded and the recording stored in high-security storage.	X; requirement in Identifier Governance Framework			
3. All GLEIF Controllers MUST mutually authenticate each other's legal identities before proceeding with any futher steps. An example is each Controller visually presenting one or more legal identity credentials for all other Controllers to verify against the list of initial GLEIF Controllers.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
4. Creation of GLEIF Root AID	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
The following steps MUST be performed in the order listed and completed during this OOBI session for the GLEIF Root AID.				
a. Each GLEIF Root AID Controller MUST generate its own single signature AID that is a participating member in the group of AIDs that will be used to create the GLEIF Root AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
b. Each GLEIF Controller MUST use an OOBI protocol (such as a QR code or live chat) to share its own AID and Service Endpoints with the other Controllers. For each GLEIF Controller, this provides the participating AID and the service endpoint whereby the other Controllers may obtain the Key Event Log (KEL) of its participating AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
c. Each GLEIF Controller MUST send a Challenge Message to every other GLEIF Controller as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of their Controller AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Operations
d. Each GLEIF Controller MUST verify in real time that a response to the Challenge Message was received from every other Controller.	X; requirement in Identifier Governance Framework			
e. Each GLEIF Controller MUST verify the signature of every other Controller.	X; requirement in Identifier Governance Framework			
f. One of the GLEIF Controllers MUST be designated as the GLEIF Genesis Controller.	X; requirement in Identifier Governance Framework			
g. The GLEIF Genesis Controller MUST select the AIDs and Service Endpoints from the GLEIF Root AID Witness Pool.	X; requirement in Identifier Governance Framework			
h. Using the current public key and the next public key digest from each of the participating AID Inception Events and the Root Witness AIDs, the GLEIF Genesis Controller MUST generate the GLEIF Root AID Inception Event and publish this to the other Controllers and to the Root AID Witnesses designated by that Inception Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
i. Each GLEIF Controller MUST verify the set of public keys, the next public key digest, and Witness identifiers in the Root AID Inception Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
j. Each Controller MUST verify the set of service endpoints for the Root AID Witnesses.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
k. Each Controller MUST sign and publish to the Root AID Witnesses their signature on the Root AID Inception Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
l. Each Controller MUST verify that the Root AID Inception Event is fully witnessed by every Root AID Witness.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
5. Creation of the GLEIF Delegated AIDs				
The following steps MUST be performed in the order listed and completed during this OOBI session for each of the two GLEIF Delegated AIDs.				
a. Each GLEIF Delegated AID Controller that is a participating member in the group of AIDs MUST generate its own single signature AID that will be used to create the GLEIF Delegated AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations

b. Each GLEIF Delegated AID Controller MUST use an OOBI protocol (such as a QR code or live chat) to share its own AID and Service Endpoints with the other Controllers. For each Controller, this provides the participating AID and the service endpoint whereby the other Controllers may obtain the KEL of its participating AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
c. Each Controller MUST send a Challenge Message to every other Controller as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of their Controller AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Operations
d. Each Controller must verify in real time that a response to the Challenge Message was received from every other Controller.	X; requirement in Identifier Governance Framework			
e. Each Controller must verify the signature of every other Controller.	X; requirement in Identifier Governance Framework			
f. One of the Controllers must be designated as the GLEIF Delegated AID Genesis Controller.	X; requirement in Identifier Governance Framework			
g. The GLEIF Delegated AID Controller MUST select the AIDs and Service Endpoints from the GLEIF Delegated AID Witness Pool.	X; requirement in Identifier Governance Framework			
h. Using the current public key and the next public key digest from each of the participating AID Inception Events, the Delegated Witness AIDs, and the GLEIF Root AID, the GLEIF Delegated AID Genesis Controller MUST generate the GLEIF Delegated AID Inception Event and publish this to the other Controllers and to the Delegated AID Witnesses designated by that Inception Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
i. Each Controller MUST verify the set of public keys, the next public key digest, the Witness identifiers and the Root AID in the Delegated AID Inception Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
j. Each Controller MUST verify the set of Witness endpoints for the GLEIF Delegated AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
k. Each Controller MUST sign and publish to the Delegated AID Witnesses their signature on the Delegated AID Inception Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
l. Each Controller MUST verify that the Delegated AID Inception Event is fully witnessed by every Witness.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
6. Rotation Event to delegate the GLEIF Delegated AIDs				
a. The set of GLEIF Root AID Controllers MUST each rotate their participating AIDs.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
b. Using the current public key, the next public key digest from each of the participating AID Rotation Events, and the digests of the GLEIF Delegated AID Inception Event, the GLEIF Genesis Controller MUST generate a GLEIF Delegated AID Rotation Event and publish this to the other Controllers and to the Root AID Witnesses.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
c. Each GLEIF Controller 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 Key Mangement
d. Each GLEIF Controller MUST sign and publish to the Root AID Witnesses their signature on the Root AID Rotation Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
e. Each GLEIF Controller MUST verify that the Root AID Rotation Event is fully witnessed by every Witness.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
7. Creation of QVI Delegated AIDs				
The following steps MUST be performed in the order listed and completed during an OOBI session for a given QVI Delegated AID.				
a. Each QVI Delegated AID Controller that is a participating member in the group of AIDs MUST generate its own single signature AID that will be used to create the QVI Delegated AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
b. Each QVI Delegated AID Controller MUST use an OOBI protocol (such as a QR code or live chat) to share its own AID with the other Controllers. For each Controller, this provides the participating AID and the service endpoint whereby the other Controllers may obtain the KEL of its participating AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
c. Each Controller MUST send a Challenge Message to every other Controller as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of their Controller AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Operations
d. Each Controller must verify in real time that a response to the Challenge Message was received from every other Controller.	X; requirement in Identifier Governance Framework			
e. Each Controller must verify the signature of every other Controller.	X; requirement in Identifier Governance Framework			
f. One of the Controllers must be designated as the QVI Delegated AID Genesis Controller.	X; requirement in Identifier Governance Framework			
g. Using the current public key and the next public key digest from each of the participating AID Inception Events, the Delegated Witness AIDs, and the GLEIF External Delegated AID, the QVI Delegated AID Genesis Controller MUST generate the QVI Delegated AID Inception Event and publish this to the other Controllers and to the Delegated AID Witnesses designated by that Inception Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
h. Each Controller MUST verify the set of public keys, the next public key digest, the Witness identifiers and the GLEIF External Delegated AID in the Delegated AID Inception Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
i. Each Controller MUST verify the set of Witness endpoints for the QVI Delegated AID.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
j. Each Controller MUST sign and publish to the Delegated AID Witnesses their signature on the Delegated AID Inception Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
k. Each Controller MUST verify that the Delegated AID Inception Event is fully witnessed by every Witness.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
8. Interaction Event to delegate QVI Delegated AIDs				
a. GLEIF MUST designate on of the GLEIF External Delegated AID Controllers as the GLEIF External AID Interaction Event Controller.	X; requirement in Identifier Governance Framework			
b. Using the current public key from each of the participating AID Controllers and the digest of the QVI Delegated AID Inception Event, the GLEIF External AID Interaction Event Controller MUST generate a GLEIF Delegated AID Interaction Event and publish this to the other Controllers and to the GLEIF Delegated AID Witnesses.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
c. Each Controller MUST verify the delegated Inception Event digest in that Interaction Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
d. Each Controller MUST sign and publish to the GLEIF Delegated AID Witnesses their signature on the GLEIF Delegated AID Interaction Event.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
e. Each Controller MUST verify that the GLEIF Delegated AID Interaction Event is fully witnessed by every Witness.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations
9. Rotation Event to delegate QVI Delegated AIDs				
a. The set of GLEIF External Delegated AID Controllers MUST each rotate their participating AIDs.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Identifier Operations

b. GLEIF MUST designate on of the GLEIF External Delegated AID Controllers as the GLEIF External AID Rotation Event Controller.	X; requirement in Identifier Governance Framework			
c. Using the current public key, the next public key digest from each of the participating AID Rotation Events, and the digest of the QVI Delegated AID Inception Event, the GLEIF External AID Rotation Event Controller MUST generate a GLEIF Delegated AID Rotation Event and publish this to the other Controllers and to the GLEIF Delegated AID Witnesses.	X; requirement in Identifier Governance Framework			X; covered as part of KERI Key Mangement
d. Each Controller 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 Key Mangement
e. Each Controller 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
e. Each Controller 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				
1. The GLEIF Root AID and GLEIF Delegated Internal and External AIDs MUST be published in a sufficiently strongly correlated and fault-tolerant manner to establish it as the unique AID for GLEIF.	X; requirement in Identifier Governance Framework			
2. The set of publication points MUST include at least the following:	X; requirement in Identifier Governance Framework			
a. The GLEIF HTTPS website.	X; requirement in Identifier Governance Framework			
b. The HTTPS websites of at least ten members of the GLEIF Regulatory Oversight Committee.	X; requirement in Identifier Governance Framework			
c. The HTTPS websites of all QVIs.	X; requirement in Identifier Governance Framework			
d. In the KERI Event Log for all GLEIF KERI Witnesses.	X; requirement in Identifier Governance Framework			
e. Published to at least 3 international newspapers in separate national jurisdictions.	X; requirement in Identifier Governance Framework			
f. Published to public registries (to be specified).	X; requirement in Identifier Governance Framework			
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			
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

	Requirement satisfied by vLEI Ecosystem Governance Framework	Requirement to be satisfied by ISO 20000 Certification	Requirement satisfied by vLEI Issuer Qualification Program	Requirement satisfied by KERI Operations
MUST' Statements Qualfied vLEI Issuer vLEI Credential (QVI vLEI Credential)				
The Issuer MUST:				
1. ensure that the Issuer of the QVI vLEI Credentials is GLEIF.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
2. for initial issuance, confirm that the QVI successfully has completed the vLEI Issuer Qualification Program and has been issued a QVI vLEI Credential.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
3. confirm that the QVI successfully has completed Annual Qualification and continues to hold a valid QVI Credential.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
The Issuer MUST:				
1. use the QVI vLEI Credential schema defined in section 8.1.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; Credential format in KERI code
2. include the Claims marked as Required in section 8.1.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; Credential format in KERI code
QVI Idenity Verification				
1. Identity Assurance				
a. A GLEIF Authorized Representative (GAR) MUST perform identity assurance of a person serving in the role of QVI Authorized Representative (QAR) to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html)	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for GLEIF	
2. Identity Authentication				
a. A credential wallet MUST be set up for the QVI.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer	
b. The QVI MUST designate a QAR to act on its behalf.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer	
c. A 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 webmeeting attended by all parties on both audio and video.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
d. The following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
i. The GAR MUST perform manual verification of the QAR's legal identity for which the GAR has already performed Identity Assurance. An example is the QAR visually presenting one or more legal identity credentials and the GAR compares the credentials verified during Identity Assurance to the QAR Person.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for GLEIF	
ii. The GAR MUST use an OOBI protocol (such as a QR code or live chat) to share the GLEIF Controller External Autonomic Identifier (AID) with the QAR.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for GLEIF	
iii. An QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the GAR.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer	
iv. The GAR MUST send a Challenge Message from the GLEIF Controller External AID to the QVI AID as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of the QVI AID.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with KERI
v. The QAR MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the QAR must acknowledge that this action has been completed.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with KERI
vi. The GAR must verify in real time that the response to the Challenge Message was received from the QAR.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with KERI
vii. When the response to the Challenge Message has been received, the GAR must verify the signature of the QAR.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for GLEIF	
Issuance				
The GAR MUST approve issuance of a QVI vLEI Credential after the completion of QVI Identity Verification in section 6.3 above.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with KERI
Voluntary revocation				
a. A QAR MUST revoke a Legal Entity vLEI Credential upon receipt of a Fully Signed revocation request by the AVR(s) of the Legal Entity, e.g., if the Legal Entity chooses to no longer be the Holder of this Credential using the GLEIF-supplied vLEI software.	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential revocation process with KERI
b. A GAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
Involuntary Revocation				
Involutary revocation of vLEI Credentials MUST follow the process specified in Appendix 5, Service Level Agreement (SLA).	X; requirement in Credential Governance Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
The QVI vLEI Credential MUST contain the LEI of the QVI.	X; requirement in Credential Governance Framework			X; Credential format in KERI code
Verifier Policies				
1. When part of a chain, each chained vLEI MUST include a reference to one or more preceding vLEIs in its provenance chain.	X; requirement in Credential Governance Framework			X; covered by ACDC requirements in KERI code
2. If any preceding vLEIs in the provenance chain or a given vLEI is revoked then that given vLEI MUST not verify.				X; covered by ACDC requirements in KERI code
3. The schema for each type of vLEI defines what type or types of vLEIs MUST or MAY be referenced in its provenance section.				X; Credential format in KERI code

	Requirement satisfied by vLEI Ecosystem Governance Framework	Requirement to be satisfied by ISO 20000 Certification	Requirement satisfied by vLEI Issuer Qualification Program	Requirement satisfied by KERI Operations
MUST' Statements Legal Entity vLEI Credential				
The Issuer MUST:				
1. be a Qualified vLEI Issuer (QVI) in the vLEI Ecosystem with qualification up to date.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
2. follow all of the requirements specified in the vLEI Issuer Qualification Agreement.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
3. use the GLEIF-supplied vLEI software for hosting Witnesses, Watchers, Discovery, and Oracles, and for Key Management.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
The Issuer MUST:			X; assessment and demonstration of Qualified vLEI Issuer compliance	
1. use the Legal Entity vLEI Credential schema defined in section 8.1.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in KERI code
2. include the Claims marked as Required in section 8.1.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in KERI code
Legal Entity Identity Verification				
Identity Assurance				
a. A QVI Authorized Representative (QAR) MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the Credential has been made.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
b. A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity is Issued and Active in the Global LEI System.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
c. A QAR MUST perform identity assurance of a person serving in the role of an Authorized vLEI Representative (AVR) to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html)	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Identity Authentication				
a. A credential wallet MUST be set up for the Legal Entity.	X; requirement in Credential Governance Framework			
b. The Legal Entity MUST designate a set of one or more Authorized vLEI Representatives (AVRs) to act on its behalf.	X; requirement in Credential Governance Framework			
i. The Legal Entity SHOULD designate at least three AVRs in order to use the greater security of KERI multi-sig protocols.	X; requirement in Credential Governance Framework			
c. A QVI Authorized Representative (QAR) and the AVRs MUST establish a real-time OOBI session in which the QAR and all AVRs are present. An example is a continuous webmeeting attended by all parties on both audio and video.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
d. The following steps MUST be performed in this order and completed during this OOBI session	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
i. The QAR MUST perform manual verification of each AVR's legal identity for which the QAR has already performed Identity Assurance. An example is each AVR visually presenting one or more legal identity credentials and the QAR compares the credentials verified during Identity Assurance to the AVR Person.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
ii. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI Autonomic Identifier (AID) with the AVRs.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
iii. An AVR MUST use an OOBI protocol (such as a QR code or live chat) to share the Legal Entity AID with the QAR.	X; requirement in Credential Governance Framework			
iv. The QAR MUST send a Challenge Message to the Legal Entity AID as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of the Legal Entity AID.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
v. Each AVR MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the AVR must acknowledge that this action has been completed.	X; requirement in Credential Governance Framework			X; covered as part of the Credential issuance process with KERI
vi. The QAR must verify in real time that a response to the Challenge Message was received from each AVR.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
vii. When all responses to Challenge Messages sufficient to satisfy the multi-sig threshold have been received, the QAR must verify the complete set of signatures.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Issuance				
The Legal Entity Identity Verification process outlined in section 6.3 MUST be completed before Legal Entity vLEI Credential issuance can begin.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
GLEIF MUST implement the vLEI Reporting API to enable QVIs to report each issuance event of Legal Entity vLEI Credentials.	X; requirement in Credential Governance Framework		X; assessment and demonstration of GLEIF compliance	
QVIs MUST call the vLEI Reporting API with each issuance event of Legal Entity vLEI Credentials.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Voluntary revocation				
a. The Legal Entity MUST notify the QVI to revoke an ECR vLEI Credential upon receipt of a fully signed revocation request by the AVR(s) of the Legal Entity using the GLEIF-supplied KERI vLEI software.	X; requirement in Credential Governance Framework			X; covered as part of the Credential revocation process with KERI
b. A QAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Involuntary Revocation				
Involuntary revocation of vLEI Credentials MUST follow the process specified in Appendix 5, Service Level Agreement (SLA).	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
GLEIF MUST update the list of Legal Entity vLEI Credentials on the LEI page of the Legal Entity to reflect vLEI credential revocations that have been reported by QVIs	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
The Legal Entity vLEI Credential MUST contain the LEI of Legal Entity Holder.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in KERI code
The following text MUST appear in the Rules section of the Automatic Chained Data Container (ACDC) vLEI Credentials.	X; requirement in Credential Governance Framework			X; Credential format in KERI code
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 section 6.3 of the Credential Governance Framework were met in accordance with the vLEI Ecosystem Governance Framework.				

	Requirement satisfied by vLEI Ecosystem Governance Framework	Requirement to be satisfied by ISO 20000 Certification	Requirement satisfied by vLEI Issuer Qualification Program	Requirement satisfied by KERI Operations
MUST' Statements Legal Entity Official Organizational Role vLEI Credential (OOR vLEI Credential)				
The Issuer MUST:				
1. be a Qualified vLEI Issuer (QVI) that has been contracted by a Legal Entity holding a valid Legal Entity vLEI Credential to issue OOR vLEI redentials.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
The Issuer MUST:			X; assessment and demonstration of Qualified vLEI Issuer compliance	
1. use the OOR vLEI Credential schema defined in section 8.1. Additional schema elements may be added depending on the requirement of a use case.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in KERI code
2. include the Claims marked as Required in section 8.1.			X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in KERI code
Legal Entity Identity Verification - Identity Assurance				
a. A QVI Authorized Representative (QAR) MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the Credential has been made.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
b. A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity is Issued and Active in the Global LEI System.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
c. The QAR MUST confirm that the Legal Entity has obtained the consent of the Official Organizational Role Person (OOR Person) for the OOR Person's name and Official Organization Role to be published by GLEIF as part of the OOR vLEI Credential elements on the LEI page of the Legal Entity.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
OOR Person Identity Verification				
1. Identity Assurance				
a. A QAR MUST perform identity assurance of an OOR Person at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html).	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI (for cryptographic trust requirement)
2. Identity Authentication				
a. A credential wallet MUST be set up for the OOR Person.	X; requirement in Credential Governance Framework			
b. A QAR MUST validate the name and the Official Organizational Role of an OOR Person using one or more official public sources.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
c. If the the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the request for the issuance of the OOR vLEI Credential MUST be made by two AVRs of the Legal Entity. Example: to cover cases such as an Interim CEO for which the entity registration records of the Legal Entity may not reflect the name and role of the Interim CEO.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
d. A QAR and the OOR Person MUST establish a real-time OOBI session in which the QAR and the OOR Person are present. An example is a continuous webmeeting attended by all parties on both audio and video.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
e. The following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
i. The QAR MUST perform manual verification of the OOR Person's legal identity for which the QVI has already performed Identity Assurance. An example, the OOR Person visually presenting one or more legal identity credentials and the QAR compares the credentials verified during Identity Assurance to the OOR Person.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
ii. A QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI Autonomic Identifier (AID) with the AVRs.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
iii. The OOR Person MUST use an OOBI protocol (such as a QR code or live chat) to share the its AID with the QAR.	X; requirement in Credential Governance Framework			
iv. The QAR MUST send a Challenge Message to the OOR Person's AID as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of the OOR Person's AID.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
v. The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OOR Person MUST acknowledge that this action has been completed.	X; requirement in Credential Governance Framework			X; covered as part of the Credential issuance process with KERI
vi. The QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
vii. When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the OOR Person's signature.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
3. A workflow MUST be implemented in the operations of the QVI which requires, prior to issuing an OOR vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR and then approved separately by another QAR.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Issuance				
1. The Legal Entity and OOR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before OOR vLEI Credential issuance can begin.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
2. GLEIF MUST implement the vLEI Reporting API to enable Qualified vLEI Issuers to report each issuance event of Legal Entity Official Organizational Role vLEI Credentials.	X; requirement in Credential Governance Framework		X; assessment and demonstration of GLEIF and Qualified vLEI Issuer compliance	
A QAR MUST call the vLEI Reporting API with each issuance event of OOR vLEI Credentials for which the Legal Entity has communicated that consent has been obtained by the OOR vLEI Credential Holder.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Voluntary Revocation			X; assessment and demonstration of Qualified vLEI Issuer compliance	
a. The Legal Entity MUST notify the QVI to revoke an OOR vLEI Credential upon receipt of a fully signed revocation request by the AVR(s) of the Legal Entity using the GLEIF-supplied KERI vLEI software.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with KERI
b. A QAR MUST perform the revocation within the timeframe specified in Appendix 5, Qualified vLEI Issuer Service Level Agreement (SLA).	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
GLEIF MUST implement a vLEI Reporting API to enable QVIs to report each revocation event of OOR vLEI Credentials.	X; requirement in Credential Governance Framework		X; assessment and demonstration of GLEIF and Qualified vLEI Issuer compliance	
A QAR MUST call the OOR Reporting API with each revocation event of Legal Entity Official Organizational Role vLEI Credentials.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
GLEIF MUST update the list of OOR vLEI Credentials on the LEI page of the Legal Entity to reflect vLEI credential revocations that have been reported by QVIs.	X; requirement in Credential Governance Framework		X; assessment and demonstration of GLEIF compliance	
GLEIF MUST monitor the QVI Transaction Event Logs (TELs) to detect the issuance or revocation of OOR vLEI Credentials which were not reported using the vLEI Reporting API.	X; requirement in Credential Governance Framework		X; assessment and demonstration of GLEIF compliance	

The OOR vLEI Credential MUST contain the following elements at a minimum - the LEI of the Holder of the Legal Entity vLEI Credential, the Legal Name of the Person in the Official Role at the Legal Entity and the Official Organizational Role itself.	X; requirement in Credential Governance Framework			X; Credential format in KERI code
The following text MUST appear in the Rules section of the Automatic Chained Data Container (ACDC) vLEI Credentials.	X; requirement in Credential Governance Framework			X; Credential format in KERI code
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.				

	Requirement satisfied by vLEI Ecosystem Governance Framework	Requirement to be satisfied by ISO 20000 Certification	Requirement satisfied by vLEI Issuer Qualification Program	Requirement satisfied by KERI Operations
MUST' Statements Legal Entity Engagement Context vLEI Credential (ECG vLEI Credential)				
The Issuer MUST:				
1. be a Legal Entity holding a valid vLEI Legal Entity vLEI Credential, or be a Legal Entity holding a valid Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials to one or more QVIs, offered by QVIs as a value-added service.	X; requirement in Credential Governance Framework			
The Issuer MUST:				
1. use the ECR vLEI Credential schema elements defined in section 8.1. Additional schema elements may be added depending on the requirement of a use case.	X; requirement in Credential Governance Framework			X; Credential format in KERI code
2. include the Claims marked as Required in section 8.1	X; requirement in Credential Governance Framework			X; Credential format in KERI code
Legal Entity Identity Verification - Identity Assurance				
a. A QVI Authorized Representative (QAR) MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the Credential has been made.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
b. A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity is Issued and Active in the GIobal LEI System.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Engagement Context Role Person (ECR Person) Identity Verification - Identity Assurance	X; requirement in Credential Governance Framework			X; covered as part of the Credential issuance process with KERI
A QAR MUST perform identity assurance of an ECR Person at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html).	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Engagement Context Role Person (ECR Person) Identity Verification - Identity Authentication				
a. A credential wallet MUST be set up for the ECR Person.	X; requirement in Credential Governance Framework			
b. A QAR and the ECR Person MUST establish a real-time OOBI session in which the QAR and the OOR Person are present. An example is a continuous webmeeting attended by all parties on both audio and video.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
c. The following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in Credential Governance Framework			
i. The QAR MUST perform manual verification of the ECR Person's legal identity for which the QVI has already performed Identity Assurance. An example, the ECR Person visually presenting one or more legal identity credentials and the QAR compares the credentials verified during Identity Assurance to the ECR Person.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
ii. A QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI Autonomic Identifier (AID) with the AVRs.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
iii. The ECR Person MUST use an OOBI protocol (such as a QR code or live chat) to share the its AID with the QAR.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
iv. The QAR 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.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
v. 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.	X; requirement in Credential Governance Framework			X; covered as part of the Credential issuance process with KERI
vi. The QAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
vii. When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the ECR Person's signature.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Issuance				
The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before ECR vLEI Credential issuance can begin.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
Voluntary revocation				
a. The Legal Entity MUST notify the QVI to revoke an ECR vLEI Credential upon receipt of a Fully Signed revocation request by the AVR(s) of the Legal Entity using the GLEIF-supplied KERI vLEI software.	X; requirement in Credential Governance Framework			X; covered as part of the Credential revocation process with KERI
b. The Qualified vLEI Issuer MUST perform the revocation within the timeframe specified in the agreement that has delegated the issuance of Legal Entity Engagement Context Role vLEI Credentials to one or more Qualified vLEI Issuers, offered by Qualified vLEI Issuers as a value-added service.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
ECR vLEI Credentials for AVRs				
a. ECR vLEI Credentials MUST be issued to the AVRs of a Legal Entity.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
b. The ECR vLEI Credentials for AVRs MUST be issued by a QVI.	X; requirement in Credential Governance Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
The following text MUST appear in the Rules section of the Automatic Chained Data Container (ACDC) vLEI Credentials.	X; requirement in Credential Governance Framework			
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.				