



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Primary Document in DID URL Change History Tab

Status: Final

Section	Sub-Section	'MUST' Statements EGF Primary Document	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 vLEI Software
Principles	1.	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			
	2.	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			
	3.	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			
	4.	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
	5.	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
	6.	The vLEI Ecosystem Governance Framework MUST fulfill GLEIF's intention to make the vLEI infrastructure widely available as 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
	7.	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
	8.	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
	9.	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; covered as part of the Credential verification process
	10.	The vLEI Ecosystem Governance Framework MUST allow vLEI Ecosystem stakeholders to be accountable to each other for conformance to the purpose, principles, and policies of the vLEI Ecosystem Governance Framework. All vLEI Ecosystem stakeholders MUST be responsible and be able to demonstrate compliance with any other requirements of applicable law. Nothing in the vLEI Ecosystem Governance Framework SHOULD require vLEI Ecosystem stakeholder to breach applicable law in order to perform its obligations under the vLEI Ecosystem Governance Framework.		X; annual certification	X; confirmation during Annual vLEI Issuer Qualification for both Qualified vLEI Issuer and GLEIF	
General Requirements	1.	All LEIs contained in vLEIs MUST maintain an LEI Entity Status of Active and an LEI Registration Status of Issued, Pending Transfer or Pending Archival in the Global LEI System.	X; requirement in Credential Frameworks	X; check using GLEIF API	X; check using GLEIF API	
	2.	All Issuers of vLEIs 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
	3.	All 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.	vLEIs 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 Framework when providing vLEI services to a QVI.			X; documentation provided by Qualified vLEI Issuers	
Revisions	1.	At a minimum, the vLEI Ecosystem Governance Framework MUST be reviewed annually.		X; GLEIF process monitoring		
	3.a.	All revisions to the Primary Document MUST be identified with a revision number that is a sequential integer.		X; follow revision requirements		
	4.a.	All revisions to Controlled Documents MUST be identified with a revision number that is a sequential integer.		X; follow revision requirements		
	5.	All revisions to the vLEI Ecosystem Governance Framework MUST be approved by GLEIF using its Change Management Process.		X; follow process requirements		



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Information Trust Policies in DID URL Change History Tab

Status: Final

Section	Sub-section	'MUST' Statements Information Trust Policies	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 vLEI Software
3 Regulatory Compliance	2.	vLEI Ecosystem stakeholders 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 or standards organizations (e.g., EU General Data Protection Regulation (GDPR), ISO/IEC 27001 – Information Security Management)).	X; although GLEIF will not be able to determine compliance by Ecosystem stakeholders other than itself and Qualified vLEI Issuers			
4 vLEI Ecosystem Stakeholder Privacy Policies	2.	The vLEI Ecosystem Credential Governance Frameworks MUST specify the information 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 stakeholders other than itself and Qualified vLEI Issuers			
5 vLEI Ecosystem Stakeholder Data Protection Policies	1.	vLEI Ecosystem stakeholders 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 stakeholders 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 stakeholders 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 stakeholders 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 are implemented and enforced.			X; confirmation during Annual vLEI Issuer Qualification	
	5.	When a privacy breach is suspected, the involved vLEI Ecosystem stakeholders 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 stakeholders other than itself and Qualified vLEI Issuers		X; confirmation during Annual vLEI Issuer Qualification	
	6.	Qualified vLEI Issuers MUST document privacy breaches in an Incident Report .			X; Incident reports filed by Qualified vLEI Issuers for all privacy breaches	
6 vLEI Ecosystem Stakeholder Security Policies	1.	vLEI Ecosystem stakeholders MUST publish, review annually, maintain, and comply with IT security policies and practices sufficient to protect all services that a vLEI Ecosystem stakeholder 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 stakeholders 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 stakeholder involved with vLEI Transactions or vLEI Data. The vLEI Ecosystem stakeholder 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 stakeholders 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 stakeholder 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 stakeholders 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	
7 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. GLEIF and the Qualified vLEI Issuers will handle through the Incident Management process. Please refer to section 5, Incident Management, of Appendix 5: Qualified vLEI Issuer Service Level Agreement, for the detailed Incident Management process.			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	
8 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	
9 Developer Security Policies	1.	When designing software or services or implementing technical changes/upgrades to vLEI software, developers of Qualified vLEI Issuers, MUST follow the security recommendations in the following specifications using the links to access the current versions:			X; confirmation during Annual vLEI Issuer Qualification	
	a.	For the Key Event Receipt Infrastructure (KERI) specification https:// trustoverip .github .io/ kswg -keri -specification			X; confirmation during Annual vLEI Issuer Qualification	
	b.	For the Authentic Chained Data Container (ACDC) specification https:// trustoverip .github .io/ kswg -acdc -specification			X; confirmation during Annual vLEI Issuer Qualification	
	c.	For the Composable Event Streaming Representation (CESR) specification https:// trustoverip .github .io/ kswg -cesr -specification			X; confirmation during Annual vLEI Issuer Qualification	



Spreadsheet Version Date: March 25, 2026

Status: Final

Section	Sub-section	There are no 'MUST' Statements in the Governance Requirements Controlled Document.	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 vLEI Software



Spreadsheet Version Date: 2022-12-16

Status: Final

Section	Sub-section	'MUST' Statements Business Requirements	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 vLEI Software
1 Business Requirements	3.	X; although GLEIF will not be able to determine compliance by Ecosystem stakeholders other than itself and Qualified vLEI Issuers	X	X	X	
	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		X	
	6.	The QVI MUST ensure that its operations regarding vLEIs are sustainably financed.	X		X	
	7.	GLEIF MUST not contribute funds of any form whatsoever for QVI operations.	X		X	



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Technical Requirements Part 1: KERI Infrastructure in DID URL Change History Tab

Status: Final

Section	Sub-section	'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 vLEI Software
1. KERI Specifications						
1.2 Specification Version Upgrades	1.	Previous versions explicitly cited by policies in this document MUST be supported for a period 18 months .	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	
2. Backer Management						
2.1 Witness Pool:		A Witness Pool:				
	1.	MUST use KERI's Algorithm for Witness Agreement (KAWA);	X		X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
	2	MUST maintain a sufficient majority threshold on a minimum pool of 5 Witnesses;	X		X; assessment and demonstration of compliance	
	4.	MUST publish Witnesses to at least one ecosystem discovery mechanism:	X		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 OOBIs (out-of-band-introduction) to witness or witnesses	X			
	b.	Publish OOBIs for witnesses on web site(s) discoverable by search engines.	X		X; assessment and demonstration of compliance	
	c.	Ledgers	X		X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
2.2 Registrar (Ledger):		A Registrar (Ledger):	X		X; assessment and demonstration of compliance	
	2.	MUST use a GLEIF Approved DID Method (one for each authorized ledger):	X		X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
	a.	Security guarantees are based on the particular ledger	X			X; covered by KERI Key Management Architecture
	b.	A DID method MUST be approved down to the ledger-specific level	X			X; covered by KERI Key Management Architecture
	c.	The only GLEIF Approved DID Method is did:webs.	X			
2.3 Hybrid (Witness Pool and Ledger Registrar):		A Hybrid (Witness Pool and Ledger Registrar):				
	1.	MUST use only one type for any KEL.	X			X; covered by KERI Key Management Architecture

4 Key Management						
4.1 Key-pair creation and storage infrastructure		All key-pairs MUST be generated using a cryptographic algorithm with approximately 128 bits of cryptographic strength. This includes using a source of entropy of approximately 128 bits of cryptographic strength for the salt or seed used to generate the private key of the key pair.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
	4.1.1 Strength					
	4.1.2 Autonomic Identifiers (AIDs)	Both Authentic Chained Data Container (ACDC) Issuer and Issuee AIDs MUST be transferable.	X			X; covered by KERI Key Management Architecture
	4.1.3 Key Pre-Rotation for Transferable AIDs 1.					
	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			X; covered by KERI Key Management Architecture
	2.	Non-delegated pre-rotated keys are at the root level of a delegation hierarchy and MUST have the very highest level of protection. There is no recovery mechanism within KERI to regain control over a non-delegated AID once its pre-rotated keys have been captured. The only recourse is to abandon the AID and stand up a new AID and reestablish the reputation and associations of the new AID. This re-establishment process is ecosystem dependent and is not part of KERI.	X			
4.2 Signature Creation Infrastructure		Another layer of protection is provided by the Witness pool which MUST endorse all events.	X			
4.3 Signature Verification Infrastructure		Best practices for code delivery and library usage MUST be observed for signature verification infrastructure. Because the signature verification infrastructure need never be publicly disclosed an attacker must first discover what computing devices are being used to verify signatures.	X			
	1.					
5 GLEIF KERI Profile						
5.1 GLEIF Root AID Inception Event						
	1.	1. GLEIF MUST hold a recorded GLEIF Root AID Genesis Event with at least a minimum of three Witnesses.	X		X; assessment and demonstration of GLEIF compliance	
	2.	The OOB for 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			
	i.	EU-FI-HTZ-01 65.21.253.212 Prod 1 Helsinki	X			
	ii.	NA-CA-OVH-01 51.79.54.121 Prod 1 Canada	X			
	iii.	AF-ZA-AZR-01 102.37.159.99 Prod 1 South Africa	X			
	iv.	SA-BR-AWS-01 54.233.109.129 Prod 1 Brazil	X			
	v.	AS-CN-ALI-01 8.210.213.186 Prod 1 China	X			
	vi.	OC-AU-OVH-01 51.161.130.60 Prod 2 Sydney	X			
	vii.	NA-US-HTZ-01 5.161.49.239 Prod 2 Ashburn	X			
	viii.	AS-JP-AZR-01 20.78.61.227 Prod 2 Japan	X			
	ix.	AF-ZA-AWS-01 13.244.119.106 Prod 2 South Africa	X			
	x.	EU-UK-ALI-01 8.208.27.153 Prod 2 United Kingdom	X			
	b.	MUST be stored at HTTPS URLs of the following affiliated organizations:	X			
	i.	Qualified vLEI Issuers	X			
	c.	MUST be stored as a file on a public GLEIF GitHub repository.	X			
	d.	MUST be shared on the following social media:				
	i.	LinkedIn and X (formerly Twitter)	X			
5.2 GLEIF Root AID						
	1.	Non-delegated pre-rotated keys are at the root level of the delegation hierarchy and MUST have the very highest level of protection.	X			X; covered by KERI Key Management Architecture
	2.	The GLEIF Root AID MUST be a threshold multi-sig with weighting requirements that have been determined by GLEIF.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
	3.	Key Pair Creation and Storage Infrastructure MUST be within a TEE.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture

	4.	Each key-pair in a thresholded multi-sig MUST use a non-co-located TEE.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
5.3 GLEIF Root Witness Pool	1.	The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAWA.	X		X; assessment and demonstration of GLEIF compliance	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 KAWA (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)	X		X; assessment and demonstration of GLEIF compliance	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 KAWA.	X		X; assessment and demonstration of GLEIF compliance	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 KAWA.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
	5.	GLEIF Root Witness Signing Key Pair key store MAY reside on the Witness Service host but MUST use dedicated user only permissions on the key store directory and its contents.	X		X; assessment and demonstration of GLEIF compliance	
	6.	The secrets in the key store MUST be encrypted with the key loaded dynamically whenever the Witness service is started.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
	7.	The key store MUST reside on a different device or host from that of the Witness service.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
5.6 GLEIF Witness Network	1.	GLEIF MUST set up and maintain its own Witness pool.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
5.7 GLEIF Watcher Network	2.	Larger pool sizes MUST use KAWA sufficient majority thresholds.	X		X; assessment and demonstration of GLEIF compliance	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		X; assessment and demonstration of GLEIF compliance	
	5.	When used, the encryption key store MUST reside on a different device or host from that of the Watcher service.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
5.8 GLEIF Key Management	1.	The specific holders of cryptographic keys MUST be kept confidential and shall be determined by GLEIF internal policy.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
	3.	Signing keys MUST be rotated whenever there is a likelihood of key compromise.	X		X; assessment and demonstration of GLEIF compliance	
	4.	The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
	5.	Encryption keys protecting private keys SHOULD be rotated prophylactically at least quarterly and MUST be rotated whenever the associated signing key store host configuration changes.	X		X; assessment and demonstration of GLEIF compliance	
	6.	GLEIF policies for approving rotation of the issuing keys for the GLEIF-Delegated issuing identifier:	X			
	a.	MUST use an OOB (out-of-band) MFA (multi-factor authorization) mechanism to approve Delegated AID rotation.	X		X; assessment and demonstration of GLEIF compliance	X; covered by KERI Key Management Architecture
6. Qualified vLEI Issuer KERI Profile						
6.2 Delegated AIDs	1.	For added security, Qualified vLEI Issuers:	X		X; confirmation during Annual vLEI Issuer Qualification	
	a.	MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.	X		X; confirmation during Annual vLEI Issuer Qualification	
	b.	MUST use at least multi-sig scheme of at least 3 signers with a threshold of 2.	X		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		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
6.3 QVI Endorser Support: Witness Pool or Ledger Registrar		An Endorser MUST use either a Witness Pool or a Ledger Registrar for Endorsement.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
6.3.1 QVI Witness Pool	1.	The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAWA.	X		X; confirmation during Annual vLEI Issuer Qualification	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 KAWA (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)			X; confirmation during Annual vLEI Issuer Qualification	

	3	The number of Witnesses on any single continent MUST be less than the sufficient threshold as per KAWA.			X; confirmation during Annual vLEI Issuer Qualification	
	4	The number of Witnesses in any single political jurisdiction MUST be less than the sufficient threshold as per KAWA.			X; confirmation during Annual vLEI Issuer Qualification	
	7	The encryption key store MUST reside on a different device or host from that of the Witness service.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Technical Requirements Part 2: vLEI Credentials in DID URL Change History Tab

Status: Final

Section	Sub-section	'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	Requirement satisfied by vLEI Software
1 Credential Specifications						
1.2 Specification Version Upgrades	1.	Previous versions explicitly cited by policies in this document MUST be supported for a period 18 months .	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			
2 Security and Privacy	1.	All signatures for the vLEI Credentials MUST use Ed25519 Signatures CESR Proof Format.				X; covered as part of vLEI software
	2.	All vLEI Credential schema MUST be SIS compliant.				X; covered as part of vLEI software
	3.	All instantiated vLEI Credentials MUST be ACDC compliant.				X; covered as part of vLEI software
	4.	All SAIDs MUST use the cryptoBlake3-256 digest.				X; covered as part of vLEI software
3 Requirements for vLEI ACDCs	1.	Issuer and Holder Identifiers MUST be KERI AIDs.				X; covered as part of vLEI software
	2.	All vLEI Credentials MUST support JSON serialization.				X; covered as part of vLEI software
	3.	All vLEI Credentials MUST include a SAID (as evidence of immutability).				X; covered as part of vLEI software
	4.	The following ACDC sections MUST include a SAID - Attribute (data payload) section, Schema section and Rules section.				X; covered as part of vLEI software
	6.	All source links MUST include the SAID of the referenced ACDC.				X; covered as part of vLEI software
	8.	Issuers MUST support the issuance of vLEI Credentials in any or all three forms.	X		X	X; covered as part of vLEI software
	9.	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	X; covered as part of vLEI software
4 vLEI Credential Schema	1.	vLEI Credential schema MUST be compliant the SAID specification.				X; covered as part of vLEI software
	2.	All vLEI Credential schema MUST include a SAID (as evidence of immutability).				X; covered as part of vLEI software
	3.	Each vLEI Credential MUST be in compliance with its specific vLEI Credential Governance Framework.	X			X; covered as part of vLEI software
	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.				X; covered as part of vLEI software
5 Composable Event Streaming Representation (CESR)	1.	The Proof Format for vLEI credentials MUST comply with the Composable Event Streaming Representation (CESR) specification.				X; covered as part of vLEI software
6 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) section of the ACDC specification.	X			X; covered as part of vLEI software

7 Exchange Protocols	1.	vLEI credential Issuers MUST comply with the Issuance Exchange Protocol Specification (IPEX) section of the ACDC specification.	X			X; covered as part of vLEI software
-------------------------	----	---	---	--	--	-------------------------------------



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Technical Requirements Part 3: vLEI Credential Registry in DID URL Change History Tab

Status: Final

Section	Sub-section	'MUST' Statements Technical Requirements Part 3: vLEI Credential Schema Registry	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 vLEI Software
2. Official vLEI Credential Schema	2.1 Requirements					
	1.	The digest algorithm employed for generating schema SAIDs MUST have an approximate cryptographic strength of 128 bits.	X			X; covered as part of vLEI software
	2.	The SAID MUST be generated in compliance with the Self-addressing Identifiers (SAIDs) specification and MUST be encoded using CESR. The CESR encoding indicates the type of cryptographic digest used to generate the SAID.	X			X; covered as part of vLEI software
	3.	The schema MUST be JSON-Schema 2020-12 compliant. The table in 2.3 below provides the normative SAIDs for each of the official schema.	X			X; covered as part of vLEI software
	2.2 Versioning					X; covered as part of vLEI software
	1.	As per the semantic versioning rules, a backward incompatible schema MUST have a higher MAJOR version number than any backward incompatible version.	X			X; covered as part of vLEI software



Spreadsheet Version Date: 2022-12-16

Status: Final

Section	Sub-section	'MUST' Statements for GLEIF Identifier 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 vLEI Software
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 GLEIF Identifier Governance Framework			X; covered as part of KERI Key Management
	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 GLEIF Identifier Governance Framework			X; covered as part of KERI Key Management
	3.	The cryptographic digest MUST have at least 128 bits of cryptographic strength.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of KERI Key Management
6 AID Controllers	1.	All Controllers MUST establish their own Private Key Store.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of KERI Key Management
	2.	All Controllers MUST keep their private keys secret.	X; requirement in GLEIF Identifier Governance Framework			
	3.	A given Controller MUST control one and only one key pair from each set of keys.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of KERI Key Management
	4.	The KERI protocol MUST be used to transfer control authority from one set of keys to another.	X; requirement in GLEIF 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 Agents.	X; requirement in GLEIF 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 GLEIF Identifier Governance Framework			
	b.	Which Controllers shall control the GLEIF Root AID, the GIDA and the GEDA.	X; requirement in GLEIF 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 GLEIF Identifier Governance Framework			
	2.	GLEIF MUST establish real-time Out-of-Band Interaction (OOBI) session(s) in which all initial GLEIF Controllers are present. An example is a continuous web meeting attended by all parties on both audio and video. The essential feature is that there is a mutual live presentation by all participants that verifies their live participation in the session.	X; requirement in GLEIF Identifier Governance Framework			
	a.	Each session MUST be recorded and the recording stored in high-security storage.	X; requirement in GLEIF Identifier Governance Framework			
	3.	All GLEIF Controllers MUST mutually authenticate each other's legal identities before proceeding with any further 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 GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	5. Creation of GLEIF Root AID		The following steps MUST be performed in the order listed and completed during each OOBI session for the GLEIF Root AID.			
	a.	Each Root AID GLEIF Authorized Representative (Root GAR) 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 GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	b.	Each Root GAR MUST use an OOBI protocol (such as a QR code or live chat) to share its own AID and Service Endpoints with the other Root GARs. For each Root GAR, this provides the participating AID and the service endpoint whereby the other Root GARs may obtain the Key Event Log (KEL) of its participating AID.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
c.	Each Root GAR MUST send a Challenge Message to every other Root GAR as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of their Root GAR AID. The Challenge Message MUST be unique to each OOBI session.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software	

	d.	Each Root GAR MUST verify in real time that a response to the Challenge Message was received from every other Root GAR.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	e.	Each Root GAR MUST verify the signature of every other Root GAR.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	f.	One of the Root GARs MUST be designated as the Root AID GLEIF Authorized Representative Lead (Root GAR Lead).	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	g.	The Root GAR Lead MUST select the AIDs from the set of Root GARs 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 set and threshold of participants.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	h.	The Root GAR Lead MUST select the AIDs and Service Endpoints for the GLEIF Root AID Witness Pool.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	i.	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 Root GAR Lead MUST generate the GLEIF Root AID Inception Event and publish this to the Root GARs and to the Root AID Witnesses designated by that Inception Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	j.	Each Root GAR MUST verify the set of public keys, the next public key digest, the threshold, the next threshold and Root AID Witness identifiers in the Root AID Inception Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	k.	Each Root GAR MUST verify the set of service endpoints for the Root AID Witnesses.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	l.	Each Root GAR MUST sign and publish to the Root AID Witnesses their signature on the Root AID Inception Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	m.	Each Root GAR MUST verify that the Root AID Inception Event is fully witnessed by every Root AID Witness.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	n.	Each Root GAR MUST verify that the Root AID Inception Event is fully witnessed by every Root AID Witness.				
	6. Creation of GLEIF Internal Delegated AIDs	The following steps MUST be performed in the order listed and completed during each OOB session for each of the two GLEIF Delegated AIDs, namely, the GLEIF Internal Delegated AID (GIDA) in this section and the GLEIF External Delegated AID (GEDA) in section 7.				
	a.	Each Internal Delegated AID GLEIF Authorized Representative (Internal GAR) that is a participating member in the group of AIDs MUST generate its own single signature AID that will be used to create the GIDA.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	b.	Each Internal GAR MUST use an OOB protocol (such as a QR code or live chat) to share its own AID and Service Endpoints with the other Internal GARs. For each Internal GAR, this provides the participating AID and the service endpoint whereby the other Internal GARs may obtain the KEL of its participating AID.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	c.	Each Internal GAR MUST send a Challenge Message to every other Internal GAR as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of their GIDA. The Challenge Message MUST be unique to each OOB session.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	d.	Each Internal GAR MUST verify in real time that a response to the Challenge Message was received from every other Internal GAR.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	e.	Each Internal GAR MUST verify the signature of every other Internal GAR.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	f.	One of the Internal GARs MUST be designated as the Internal Delegated AID GLEIF Authorized Representative (Internal GAR Lead).	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	g.	The Internal GAR Lead MUST select the AIDs and Service Endpoints from the GLEIF Internal Delegated AID Witness Pool.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	h.	The Internal GAR Lead MUST select the AIDs from the set of Internal GARs 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 set and threshold of participants.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	i.	Using the current public key and the next public key digest from each of the participating AID Inception Events, the Internal Delegated Witness AIDs, and the GLEIF Root AID, the Internal GAR Lead MUST generate the GLEIF Internal Delegated AID Inception Event and publish this to the Internal GARs and to the Delegated AID Witnesses designated by that Inception Event. The published Inception Event includes as an attachment OOBs for each of the Internal Delegated AID Witnesses.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	j.	Each Internal GAR MUST verify the set of public keys, the next public key digest, the Witness identifiers, the threshold, the next threshold and the Root AID in the Internal Delegated AID Inception Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	k.	Each Internal GAR MUST verify the set of Witness endpoints for the GIDA.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software

	l.	Each Internal GAR MUST sign and publish to the Internal Delegated AID Witnesses its signature on the Internal Delegated AID Inception Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	m.	Each Internal GAR MUST verify that the Internal Delegated AID Inception Event is fully witnessed by every Witness.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	7. Creation of GLEIF External Delegated AIDs					
	a.	Each External Delegated AID GLEIF Authorized Representative (External GAR) that is a participating member in the group of AIDs MUST generate its own single signature AID that will be used to create the GEDA.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	b.	Each External GAR MUST use an OOB protocol (such as a QR code or live chat) to share its own AID and Service Endpoints with the other External GARs. For each External GAR, this provides the participating AID and the service endpoint whereby the other External GARs may obtain the KEL of its participating AID.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	c.	Each External GAR MUST send a Challenge Message to every other External GAR as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of their GEDA. The Challenge Message MUST be unique to each OOB session.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	d.	Each External GAR MUST verify in real time that a response to the Challenge Message was received from every other External GAR.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	e.	Each External GAR MUST verify the signature of every other External GAR.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	f.	One of the External GARs MUST be designated as the External Delegated AID GLEIF Authorized Representative Lead (External GAR Lead).	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	g.	The External GAR Lead MUST select the AIDs and Service Endpoints from the GLEIF External Delegated AID Witness Pool.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	h.	The External GAR Lead MUST select the AIDs from the set of External GARs 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 set and threshold of participants.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	i.	Using the current public key and the next public key digest from each of the participating AID Inception Events, the External Delegated Witness AIDs, and the GLEIF Root AID, the External GAR Lead MUST generate the GLEIF External Delegated AID Inception Event and publish this to the External GARs and to the Delegated AID Witnesses designated by that Inception Event. The published Inception Event includes as an attachment OOBs for each of the External Delegated AID Witnesses.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	j.	Each External GAR MUST verify the set of public keys, the next public key digest, the Witness identifiers, the threshold, the next threshold and the Root AID in the External Delegated AID Inception Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	k.	Each External GAR MUST verify the set of Witness endpoints for the GEDA.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	l.	Each External GAR MUST sign and publish to the External Delegated AID Witnesses their signature on the External Delegated AID Inception Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	m.	Each External GAR MUST verify that the External Delegated AID Inception Event is fully witnessed by every Witness.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	8. Rotation Event to delegate the GLEIF Internal Delegated AIDs	The following steps MUST be performed in the order listed and completed during this OOB session for each of the two GLEIF Delegated AIDs, namely, the GLEIF Internal Delegated AID (GIDA) in this section and the GLEIF External Delegated AID (GEDA) in section 9.				
	a.	A threshold satisfying subset of Internal GARs MUST each rotate their participating AIDs.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	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 Internal Delegated AID Inception Event, the Internal GAR Lead MUST generate a GLEIF Internal Delegated AID Rotation Event and publish this to the other participating Internal GARs and to the Root AID Witnesses.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	c.	Each Internal GAR MUST verify the set of public keys, the next public key digest, and delegated Inception Event digests in that Rotation Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	d.	Each Internal GAR MUST sign and publish to the Root AID Witnesses their signature on the Root AID Rotation Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	e.	Each Internal GAR MUST verify that the Root AID Rotation Event is fully witnessed by every Root AID Witness.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software

	9. Rotation Event to delegate the GLEIF External 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, namely, the GLEIF Internal Delegated AID (GIDA) in section 8 and the GLEIF External Delegated AID (GEDA) in this section.				X; covered as part of vLEI software
	a.	A threshold satisfying subset of External GARs MUST each rotate their participating AIDs.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	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 External Delegated AID Inception Event, the External GAR Lead MUST generate a GLEIF External Delegated AID Rotation Event and publish this to the other participating External GARs and to the Root AID Witnesses.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	c.	Each External GAR MUST verify the set of public keys, the next public key digest, and delegated Inception Event digests in that Rotation Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	d.	Each External GAR MUST sign and publish to the Root AID Witnesses their signature on the Root AID Rotation Event.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
	e.	Each External GAR MUST verify that the Root AID Rotation Event is fully witnessed by every Root AID Witness.	X; requirement in GLEIF Identifier Governance Framework			X; covered as part of vLEI software
8 Publication of GLEIF Root AID and GLEIF Delegated AIDs	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 GLEIF Identifier Governance Framework			
	2.	The set of publication points MUST include at least 4 of the list of publication points initially (highlighted below) following the creation of the GLEIF Root AID and GLEIF Delegated Internal and External AIDs.	X; requirement in GLEIF Identifier Governance Framework			
	a.	The GLEIF HTTPS website.	X; requirement in GLEIF Identifier Governance Framework			
	b.	The HTTPS website of the GLEIF Regulatory Oversight Committee.	X; requirement in GLEIF Identifier Governance Framework			
	c.	The HTTPS websites of all QVIs.	X; requirement in GLEIF Identifier Governance Framework			
	d.	In the KERI Event Log hosted by GLEIF KERI Witnesses.	X; requirement in GLEIF Identifier Governance Framework			
	e.	Published to at least 3 international newspapers in separate national jurisdictions (applies only to GLEIF Root AID). These publications are: Financial Times UK edition, South China Morning Post - Business and American Banker.	X; requirement in GLEIF Identifier Governance Framework			
	f.	Published to github repositories: The Web of Trust github repository, Public GLEIF-controlled github repository	X; requirement in GLEIF Identifier Governance Framework			
	g.	Published to public registries: IANA (IETF RFCs) registries, ISO registries	X; requirement in GLEIF 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 GLEIF 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 GLEIF Identifier Governance Framework			X; covered as part of vLEI software



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Qualified vLEI Issuer Identifier Governance Framework and vLEI Credential Framework in DID URL Change History Tab

Status: Final

Section	Sub-section	'MUST' Statements Qualified vLEI Issuer Identifier Governance Framework and vLEI Credential 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 vLEI Software
6 Issuer Policies						
6.1 Qualifications	1.	The Issuer MUST ensure that the Issuer of the QVI vLEI Credential is GLEIF.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
6.2 Credential		The Issuer MUST:				
	1.	use the QVI vLEI Credential schema defined in section 10.1.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; Credential format in vLEI software
	2.	include the Claims marked as Required in section 10.1.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; Credential format in vLEI software
6.3 Identity Verification of the Qualified vLEI Issuer Authorized Representatives (QARs)						
	1	Identity Verification (Assurance and Authentication) of each person serving in the role of QVI Authorized Representative (QAR) MUST be performed prior to the event to create the QVI Delegated AIDs. Identity Verification is a necessary process to ensure that digital identities have been verified in a secure manner to prevent impersonation, identity fraud, and ultimately, unauthorized access or use of a vLEI credential.	X			
	a.	Identity Assurance and Identity Authentication MUST be performed using a real-time Out-of-Band-Introduction (OOBI) session. An example is a continuous web meeting attended by all parties on both audio and video in which the External GLEIF Authorized Representatives (GARs) and the QARs are present.	X			
	b.	If a continuous web meeting is used for the OOBI session: i. Video filters and avatars MUST not be used during the OOBI session. ii. Passcodes and passwords MUST not be displayed on screen (shared) during the OOBI session	X			
	e.	A minimum of two QARs MUST form the QVI multi-sig group for the event to create the QVI Delegated AIDs.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	f.	If more than two QARs form the QVI multi-sig group, all of these QARs MUST participate in the event to create the QVI Delegated AIDs.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	
	d.	An External GAR MUST lead for the anchoring action for the QVI External Delegated AID described below.	X		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with vLEI software
	2. Identity Authentication					
	a.	A credential wallet MUST be set up for each QAR.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	
	b.	All of the QARs that formed the QVI multi-sig group MUST participate in the Identity Authentication.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	
	c.	An External GAR and each QAR MUST establish a continuous web meeting OOBI session in which the External GAR and the QAR are present.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software

	d.	The following steps MUST be performed in this order and completed during this OOB session.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
	i.	The External GAR MUST perform manual verification of each QAR's legal identity in the identity credential which was presented during Identity Assurance.	X		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with vLEI software
	ii.	The External GAR MUST use an OOB protocol (such as a QR code or live chat) to share the GLEIF External Delegated AID (GEDA) with each QAR.	X		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with vLEI software
	iii.	The QAR Lead MUST use an OOB protocol (such as a QR code or live chat) to share the QVI AID with the External GAR.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	iv.	The External GAR MUST send a Challenge Message from the GEDA to the QVI AID as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of the QVI AID. The Challenge Message MUST be unique to the OOB session.	X		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with vLEI software
	v.	Each QAR MUST use its Private Key Store to sign and return the response to the Challenge Message, after which each QAR MUST acknowledge that this action has been completed.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	vi.	The External GAR must verify in real time that the response to the Challenge Message was received from each QAR.	X		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with vLEI software
	vii.	When the response to the Challenge Message has been received, the External GAR must verify the signature of each QAR.	X		X; assessment and demonstration of compliance for GLEIF	
	3. Addition or Replacement of QARS					
	a.	When QVIs add or replace QARS after the issuance of the Qualified vLEI Issuer vLEI Credential, the steps within 1. Identity Assurance and Identity Authentication MUST be followed, beginning with 6.3.1.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
6.4 Creation of the QVI Delegated AIDs	1.	The creation of the QVI Delegated AIDs follows the successful completion of Identity Verification by the External GAR Lead of each QAR.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
	2.	The following steps MUST be performed in the order listed and completed during an OOB session for a given QVI Delegated AID.				
	a.	Video filters and avatars MUST not be used during the OOB session.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	
	b.	One of the QARS must be designated as the Delegated AID QVI Authorized Representative (QAR Lead).	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	c.	The QAR Lead MUST either configure or select the AIDs and Service Endpoints for the QVI Delegated AID Witness Pool.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	d.	The QAR Lead MUST select the AIDs from the set of QARS 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 set and threshold of participants.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	e.	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 GEDA, the QAR Lead MUST generate the QVI Delegated AID Inception Event and publish this to the other QARS and to the Delegated AID Witnesses designated by that Inception Event.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	f.	Each QAR MUST verify the set of public keys, the next public key digest, the Witness identifiers, the threshold, the next threshold, and the GEDA in the Delegated AID Inception Event.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	g.	Each QAR MUST verify the set of Witness endpoints for the QVI Delegated AID.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	h.	Each QAR MUST sign and publish to the Delegated AID Witnesses their signature on the Delegated AID Inception Event.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	i.	Each QAR MUST verify that the Delegated AID Inception Event is fully witnessed by every Witness.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	j.	GLEIF MUST designate one of the External GARS as the External GAR Lead.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
6.5 Delegation of the QVI Delegated AIDs	1.	Unless otherwise pre-approved by the GLEIF Root GARS, GLEIF External AID MUST use an Interaction Event to approve the delegation of the QVI Delegated AIDs.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software

	2.	The following steps MUST be performed in the order listed and completed during this OOBI session for the GLEIF External Delegated AID (GEDA).	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
		Video filters and avatars MUST not be used during the OOBI session.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
	i.	The QAR Lead initiates a set of QARs to create a multi-sig group and the QARs mutually are authenticated.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	ii.	The QAR Lead initiates the creation of the Inception Event using the published GLEIF External AID as the Delegator.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	iii.	The External GAR Lead verifies that the set of QARs in the multi-sig group in this Inception Event to delegate the QVI External AID match those that the External GAR Lead verified according to section 6.3 above.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
	iv.	The External GAR Lead submits request to the External GAR multi-sig group to anchor the Interaction event. All members of the External GAR multi-sig group trust External GAR Lead to anchor because the External GARs already have trusted the External GAR Lead to perform Identity Assurance on the QARs.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
	v.	The External GAR Lead then submits a request to issue the Qualified vLEI Issuer vLEI Credential to QVI vLEI to the External GAR multi-sig group as an Interaction Event.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
6.6 QVI vLEI Credential Issuance	1.	The External GAR MUST approve issuance of a QVI vLEI Credential after the completion of QVI Identity Verification in section 6.3 above.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
6.7 QVI vLEI Credential Revocation	1. Voluntary Revocation					
	a.	An External GAR MUST revoke a Legal Entity vLEI Credential upon receipt of a Fully Signed revocation request by the QAR(s) of the Legal Entity, e.g., if the Legal Entity chooses to no longer be the Holder of this Credential using the vLEI software.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
	b.	An External GAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
	2. Involuntary Revocation					
	a.	Involuntary revocation of vLEI Credentials MUST follow the process specified in Appendix 5, Service Level Agreement (SLA).	X		X; assessment and demonstration of compliance for GLEIF	
7 QVI Self-issuance of vLEIs	2.	GLEIF MUST oversee the assignment of these vLEI Credentials issued by QVIs to themselves.	X		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
9 Verifier Policies	2.	When part of a chain, each chained vLEI MUST include a reference to one or more preceding vLEIs in its provenance chain.	X			X; Credential format in vLEI software
	3.	If any preceding vLEIs in the provenance chain or a given vLEI is revoked, then that given vLEI MUST not verify.	X			X; Credential format in vLEI software
	4.	The schema for each type of vLEI defines what type or types of vLEIs MUST or MAY be referenced in its provenance section.	X			X; Credential format in vLEI software
10 Credential Definition						
10.1 Schema	1.	The QVI vLEI Credential MUST be an Authentic Chained Data Container (ACDC) that MUST use for its schema at the time of issuance, the JSON Schema found in: https://github.com/GLEIF-IT/vLEI-schema/blob/main/qualified-vLEI-issuer-vLEI-credential.json	X			X; Credential format in vLEI software
	2.	The field values in the credential MUST be as follows:	X			X; Credential format in vLEI software
	a.	The "LEI" field value MUST be the LEI of the QVI.	X			X; Credential format in vLEI software
	b.	The "gracePeriod" field value MUST be at least 90 (ninety) Days.	X			X; Credential format in vLEI software



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Legal Entity vLEI Credential Framework in DID URL Change History Tab

Status: Final

Section	Sub-section	'MUST' Statements Legal Entity vLEI Credential 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 vLEI Software
6 Issuer Policies		The Issuer MUST:				
6.1 Qualifications	1.	be a Qualified vLEI Issuer (QVI) in the vLEI Ecosystem with qualification up to date.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	2.	follow all of the requirements specified in the vLEI Issuer Qualification Agreement.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	3.	use the vLEI software for hosting Witnesses, Watchers and for Key Management.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	4.	The Issuer MUST be a Qualified vLEI Issuer (QVI) that has been contracted by a Legal Entity for the issuance of a Legal Entity vLEI Credential.			X; assessment and demonstration of Qualified vLEI Issuer compliance	
		The Issuer MUST:				
6.2 Credential	1.	use the Legal Entity vLEI Credential schema defined in section 9.1.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in vLEI software
	2.	include the Claims marked as Required in section 9.1.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in vLEI software
6.4. Appointment of the Legal Entity Authorized Representatives	1					
	ii.	If 2 or more LARs have been designated, the signing threshold MUST require at least 2 LARs to sign the Legal Entity vLEI Credential.				
	iv.	The Legal Entity vLEI Credential MUST be multi-signed by a threshold satisfying number of LARs before the credential can be used or presented.				
6.5. Identity Verification of the LARs	1	Identity Verification (Assurance and Authentication) of the LARs MUST be performed prior to authorization of the issuance and approval of the Legal Entity vLEI Credential. Identity Verification is a necessary process to ensure that digital identities have been verified in a secure manner to prevent impersonation, identity fraud, and ultimately, unauthorized access or use of a vLEI credential.				
	a.	Identity Assurance and Identity Authentication MUST be performed using a real-time Out-of-Band-Introduction (OOBI) session. An example is a continuous web meeting attended by all parties on both audio and video in which a QAR and the LARs are present.				
	b.	If a continuous web meeting is used for the OOBI session: i. Video filters and avatars MUST not be used during the OOBI session. ii. Passcodes and passwords MUST not be displayed on screen (shared) during the OOBI session				
	d. Identity Assurance of the LARs	1.c. Proper security access controls MUST be put in place between the QVI and the third-party provider so that the QAR can view the results of identity assurance and confirm that the persons that the third party has conducted identity assurance according to the requirements of the vLEI Ecosystem Governance Framework.				
	2. Identity Authentication of the LARs					
	a.	A credential wallet MUST be set up for the Legal Entity and for each LAR.	X			
	b.	Identity Authentication MUST be performed using a continuous web meeting OOBI session.			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		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	The QAR MUST perform manual verification of each LAR's legal identity in the identity credential which was presented during Identity Assurance.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	One of the LARs MUST be designated as the LAR Lead.				
	iii.	The LAR Lead MUST initiate the set of LARs to create a multi-sig group which will generate the AID to which the Legal Entity vLEI Credential will be issued if the AID has not been created prior to the beginning of Identity Authentication.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process vLEI software

	iv.	The QAR MUST use an OOB protocol (such as a QR code or live chat) to share the QVI Autonomic Identifier (AID) with each LAR.			X; assessment and demonstration of Qualified vLEI Issuer compliance	
	v.	Each LAR MUST use an OOB protocol (such as a QR code or live chat) to share the Legal Entity AID with the QAR.	X			X; covered as part of the Credential issuance process vLEI software
	vi.	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. The Challenge Message MUST be unique to the OOB session.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process vLEI software
	vii.	Each LAR MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the LAR MUST acknowledge that this action has been completed.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
	viii.	The QAR MUST verify in real time that a response to the Challenge Message was received from each LAR.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process vLEI software
	ix.	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		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
	3. Addition or Replacement of DARs and LARs					
	a.	When new DARs are appointed to replace or add LARs, Identity Assurance of a person serving in the role of a new DAR MUST be performed.	X			
	b.	When DARs add or replace LARs after the issuance of the Legal Entity vLEI Credential, Identity Verification of the new LAR(s) needs to be performed.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
6.4 Issuance	2	A workflow MUST be implemented in the operations of the QVI which requires two QARs to be involved in the issuance and signing a Legal Entity vLEI Credential. The first QAR creates and signs the Legal Entity vLEI credential. The second QAR then approves the issuance and signs the Legal Entity vLEI Credential as an Interaction Event.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	3	A QAR MUST send the issued Legal Entity vLEI Credential to the LARs who MUST multi-sign the Admit message to accept the credential by the Legal Entity.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	4	The QAR then MUST confirm that the LARs have Fully Signed the Admit message for the Legal Entity vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	5	A QAR MUST call the vLEI Reporting API for each issuance event of Legal Entity vLEI Credentials.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	6	GLEIF MUST update the list of vLEI Credentials on the LEI page of the Legal Entity to reflect Legal Entity vLEI credential issuances that have been reported by QVIs.	X		X; assessment and demonstration of GLEIF compliance	
6.5 Revocation	1. Voluntary Revocation					
	a.	A QAR MUST revoke a Legal Entity vLEI Credential upon receipt of a Fully Signed revocation request by the LAR(s) of the Legal Entity, e.g., if the Legal Entity chooses to no longer be the Holder of this Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with vLEI software
	b.	A QAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with vLEI software
	2.	Involuntary revocation of vLEI Credentials MUST follow the process specified in Appendix 5, Service Level Agreement (SLA).	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	3.	A QAR MUST call the vLEI Reporting API with each revocation event of Legal Entity vLEI Credentials.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	4.	GLEIF MUST update the list of vLEI Credentials on the LEI page of the Legal Entity to reflect vLEI credential revocations that have been reported by QVIs.	X		X; assessment and demonstration of GLEIF compliance	
	5.	The QAR SHOULD remove the LEI of the Legal Entity from the process to monitor the status of LEIs used within vLEIs.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	6	If the QVI has been terminated:				
	b.	Validators MUST treat as invalid any Legal Entity vLEI Credentials once the Grace Period has expired. The expiration date of the Grace Period is 90 days after the revocation date of the QVI credential.	X			
6.7 Monitoring	1.	GLEIF MUST monitor the QVI Transaction Event Logs (TEs) to detect the issuance of Legal Entity vLEI Credentials which were not reported using the vLEI Reporting API.	X		X; assessment and demonstration of GLEIF compliance	
9 Credential Definition						
9.1 Schema	1.	The Legal Entity vLEI Credential MUST be an Authentic Chained Data Container (ACDC) that MUST use for its schema at the time of issuance, the JSON Schema found in: https://github.com/GLEIF-IT/vLEI-schema/blob/main/legal-entity-vLEI-credential.json	X			X; Credential format in KERI code
	2.	The field values in the credential MUST be as follows:	X			X; Credential format in KERI code
	a.	"LEI" field value MUST be the LEI of Legal Entity Holder.	X			X; Credential format in KERI code
	3.	The Sources section MUST contain a source reference to the Qualified vLEI Issuer vLEI Credential of the QVI that issued this Legal Entity vLEI Credential.	X			X; Credential format in KERI code



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Authorization vLEI Credential Framework in DID URL Change History Tab

Status: Final

Section	Sub-section	'MUST' Statements Qualified vLEI Issuer Authorization vLEI Credential 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 vLEI Software
6 Issuer Policies						
6.1 Qualifications	1.	The Issuer MUST be a LAR of a Legal Entity that holds a valid Legal Entity vLEI Credential that was issued by the QVI with which the Legal Entity has contracted to issue vLEI Role Credentials.	X			X; covered as part of the Credential issuance process vLEI software
6.2 Credential	1.	The Issuer MUST:				
	1.	use the AUTH vLEI Credential schema defined in sections 9.1 and 9.2 for authorizing the associated OOR vLEI or ECR vLEI AUTH credentials respectively.	X			X; Credential format in vLEI software
	2.	include the Claims marked as Required in the schema indicated in 9.1 and 9.2.	X			
6.3 Issuance	1.	The LAR MUST complete the Identity Verification requirements specified in the Legal Entity Official Organizational Role (OOR) vLEI Credential Framework and the Legal Entity Engagement Context Role (ECR) vLEI Credential Framework prior to issuing OOR AUTH vLEI Credentials and ECR AUTH vLEI Credentials.				
	2.	The LAR also MUST follow the usage rules in the Legal Entity Official Organizational Role (OOR) vLEI Credential Framework for the inclusion of OOR long names, code, abbreviations and Latin Transliteration of OOR long names in creating OOR AUTH vLEI Credentials.				
	3.	The LAR MUST include the OOR Person's or ECR Person's AID obtained during Identity Verification of the OOR Person or ECR Person, as well as the name and role of the OOR Person or ECR Person, as elements within the appropriate AUTH vLEI Credential for the issuance of the associated vLEI Role Credential.				
	4.	The signatures on the AUTH vLEI Credential MUST match the signing threshold of the AID of the Legal Entity vLEI Credential				
	5.	In addition, a workflow SHOULD be implemented in the operations of a Legal Entity which requires one LAR to prepare the AUTH vLEI Credential for the issuance of a vLEI Role Credential which then is approved and signed by the remaining LARs needed to satisfy the signing threshold of the AID of the Legal Entity vLEI Credential.				
	6.	A LAR MUST issue AUTH vLEI Credential explicitly authorizing the QARs of a QVI to issue each vLEI Role Credential. The AUTH vLEI Credential will become part of the chain of the vLEI Role Credentials.				
	7.	A LAR also MUST issue an ECR AUTH vLEI Credential for ECR vLEI Credentials which the Legal Entity will issue directly.				
6.6 Monitoring	1.	GLEIF MUST monitor the QVI Transaction Event Logs (TEs) to detect revocations of QVI AUTH vLEI Credentials by LARs, at least daily. This will advise GLEIF in the case of a terminated QVI or QVI leaving the vLEI Ecosystem to follow up on revocation of any OOR vLEI Credentials.	X		X; assessment and demonstration of GLEIF compliance	
10 Credential Definition						
10.1 Schema OOR AUTH vLEI Credential	1.	The OOR AUTH vLEI Credential MUST be an Authentic Chained Data Container (ACDC) that MUST use for its schema at the time of issuance, the JSON Schema found in: https://github.com/GLEIF-IT/vLEI-schema/blob/main/oor-authorization-vlei-credential.json	X			X; Credential format in vLEI software
	2.	The field values in the credential MUST be as follows:	X			
	a.	The "AID" field value MUST be the AID of OOR Person.	X			X; Credential format in vLEI software
	b.	The "LEI" field value MUST be the LEI of Legal Entity Holder.	X			X; Credential format in vLEI software
	c.	The "personLegalName" field value MUST be the Legal Name of the Person in the Official Organizational Role at the Legal Entity as it appears in the identity credential provided by the OOR Person for Identity Assurance.	X			X; Credential format in vLEI software
	d.	The "officialRole" field value MUST be the Official Role specified in the vLEI OOR Credential.	X			X; Credential format in vLEI software
10.2 Schema ECR AUTH vLEI Credential	1.	The ECR AUTH vLEI Credential MUST be an Authentic Chained Data Container (ACDC) that MUST use for its schema at the time of issuance, the JSON Schema found in: https://github.com/GLEIF-IT/vLEI-schema/blob/main/ecr-authorization-vlei-credential.json	X			X; Credential format in vLEI software
	2.	The field values in the credential MUST be as follows:	X			X; Credential format in vLEI software
	a.	The "AID" field value MUST be the AID of ECR Person.	X			X; Credential format in vLEI software
	b.	The "LEI" field value MUST be the LEI of Legal Entity Holder.	X			X; Credential format in vLEI software
	c.	The "personLegalName" field value MUST be the Legal Name of the Person in the Engagement Context Role at the Legal Entity as it appears in the identity credential provided by the OOR Person for Identity Assurance.	X			X; Credential format in vLEI software

	d.	The "engagementContextRole" field value MUST be the Engagement Context Role specified in the vLEI ECR Credential.	X			X; Credential format in vLEI software
	3.	The Sources section MUST contain a source reference to the Legal Entity vLEI Credential (via SAID) held by the Legal Entity issuer of this credential. The Issuer of the referenced Legal Entity vLEI Credential MUST be the target holder of this ECR AUTH vLEI Credential.	X			X; Credential format in vLEI software



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Legal Entity Official Organizational Role vLEI (OOR vLEI Credential) Credential Framework in DID URL Change History Tab

Status: Final

Section	Sub-section	"MUST" Statements Legal Entity Official Organizational Role vLEI (OOR vLEI Credential) Credential 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 vLEI Software
6 Issuer Policies						
6.1 Qualifications	1.	The Issuer MUST 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 credentials.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
6.2 Credential		The Issuer MUST:				
	1.	use the OOR vLEI Credential schema defined in section 9.1. Additional schema elements may be added depending on the requirement of a use case.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in vLEI software
	2.	include the Claims marked as Required in section 9.1.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in vLEI software
6.3. Official Organizational Role (OOR) Person Identity Verification	1.	Identity Verification (Assurance and Authentication) of a person serving in an Official Organizational Role (OOR Person) MUST be performed prior to authorization of the issuance by a LAR and prior to the approval by a QAR of the issuance of an OOR vLEI Credential. Identity Verification is a necessary process to ensure that digital identities have been verified in a secure manner to prevent impersonation, identity fraud, and ultimately, unauthorized access or use of a vLEI credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	a.	Identity Assurance and Identity Authentication MUST be performed using a real-time Out-of-Band-Introduction (OOBI) session. An example is a continuous web meeting attended by all parties on both audio and video in which the LAR and the OOR Person or the QAR and the OOR Person are present.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	If a continuous web meeting is used for the OOBI session: i. Video filters and avatars MUST not be used during the OOBI session. ii. Passcodes and passwords MUST not be displayed on screen (shared) during the OOBI session.	X			
	c.	Proper security access controls MUST be put in place between the QVI and the third-party provider so that the QAR can view the results of identity assurance and confirm that the persons that the third party has conducted identity assurance according to the requirements of the vLEI Ecosystem Governance Framework.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	6.3.1. For a Legal Entity with more than one authorized signer or employee					
	1. Preparing for authorization of an OOR vLEI Credential by a LAR					
	a.	A credential wallet MUST be set up for the OOR Person.	X			
	b.i.	Identity Verification (Assurance and Authentication) of an OOR Person MUST be performed prior to authorization of the issuance of an OOR vLEI Credential if the identity of a colleague and other representative of their organizations is not well known in their role in the organization to at least one of the LARS.	X			
	c.	If Identity Assurance is performed, Identity Assurance MUST be completed prior to Identity Authentication.	X			

	d.	Identity Authentication always MUST be performed.	X			
	e.	The LAR MUST obtain the consent of the OOR Person for their name and OOR to be published on the LEI page of the Legal Entity on gleif.org . This confirmation will be indicated in the OOR Authorization vLEI Credential (OOR AUTH vLEI Credential).	X			
	f.	The LAR MUST request the OOR Person to generate its AID.	X			X; covered as part of the Credential issuance process with vLEI software
	2. Identity Authentication of an OOR Person by a LAR	Then the following steps MUST be performed in this order and completed during a continuous web meeting OOBI session.				
	a.	The LAR MUST perform manual verification of the OOR Person's legal identity in the identity credential which was presented during Identity Assurance.	X			
	b.	The LAR MUST use an OOBI protocol (such as a QR code or live chat) to share the Legal Entity AID with the OOR Person.	X			X; covered as part of the Credential issuance process with vLEI software
	c.	The OOR Person MUST use an OOBI protocol (such as a QR code or live chat) to share its AID with the LAR.	X			X; covered as part of the Credential issuance process with vLEI software
	d.	The LAR 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. The Challenge Message MUST be unique to the OOBI session.	X			X; covered as part of the Credential issuance process with vLEI software
	e.	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			X; covered as part of the Credential issuance process with vLEI software
	f.	The LAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.	X			X; covered as part of the Credential issuance process with vLEI software
	g.	When the response to the Challenge Message has been received by the LAR, the LAR MUST verify the OOR Person's signature.	X			X; covered as part of the Credential issuance process with vLEI software
	3. Preparation of the OOR AUTH vLEI Credential by the LARs					
	a.	The LAR MUST create a OOR AUTH vLEI Credential to be issued to the QVI as required in the Authorization vLEI Credential Framework.	X			
	b.	The LAR MUST follow the usage rules below for specifying OOR long names in Legal Entity OOR AUTH vLEI Credentials.	X			
	i.	The OOR long name MUST be specified in the Legal Entity OOR AUTH vLEI Credential.	X			
	ii.	If the OOR long name is included in the ISO 5009 Official Organization Role lists, then the long name of the role and its corresponding OOR code MUST be included in the Legal Entity OOR AUTH vLEI credential. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.	X			
	iii.	If the OOR long name is specified in public documents, but not in the ISO 5009 Official Organization Role lists, used by the QVI to validate the person in the role, then the role as specified in these documents MUST be included in the Legal Entity OOR AUTH vLEI credential.	X			
	iv.	If the OOR long name is specified in other documents provided by the Legal Entity, but not in the ISO 5009 Official Organization Role lists, and used by the QVI to validate the person in the role, then the role as specified in these documents MUST be included in the Legal Entity OOR AUTH vLEI credential.	X			
	g.	The OOR AUTH vLEI Credential MUST be signed by a threshold satisfying number of LARs using the Legal Entity vLEI Credential.	X			X; covered as part of the Credential issuance process with vLEI software

	4. Preparing for issuance of an OOR vLEI Credential by a QVI					
	a.	Based on the information contained in the Legal Entity OOR AUTH vLEI Credential received by the QVI:	X			
	i.	A QAR MUST validate 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 using the GLEIF API.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	ii.	A QAR MUST validate the Legal Entity Identifier (LEI) of the Legal Entity has a LEI Entity Status of Active and a LEI Registration Status of Issued, Pending Transfer or Pending Archival in the Global LEI System using the GLEIF API.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iii.	A QAR MUST validate the name and the Official Organizational Role of an OOR Person using one or more official public sources. An example of documentation that can be used to validate the name and Official Organizational Role of an OOR Person are a certified copy of documentation accessed directly by the QAR from a business registry.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iv.	If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the QAR MUST request from the LAR(s) copies of documents of the Legal Entity. Examples of documentation that can be provided by the Legal Entity to validate the name and Official Organizational Role of an OOR Person are a notarized copy of statutes or articles, Board minutes or a certificate of incumbency provided by the Legal Entity. Use of documents not certified or notarized or documents found on websites or through links provided solely by the Legal Entity are not acceptable for this validation.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	v.	If the name and the Official Organizational Role of the OOR Person cannot be validated using official public sources or copies of documents of the Legal Entity, then the QAR MUST notify the LAR that an OOR vLEI Credential cannot be issued and the LAR MAY authorize instead the issuance of an ECR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b. Identity Authentication by a QVI					
	i.	Identity Verification (Assurance and Authentication) of an OOR Person by its QVI MUST be performed prior to approval by a QAR of the issuance of an OOR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	Identity Assurance MUST be completed prior to Identity Authentication.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iii. Identity Authentication of an OOR Person by a QAR	Then the following steps MUST be performed in this order and completed during a continuous web meeting OOB session.				
	a.	A QAR MUST perform manual verification of the OOR Person's legal identity in the identity credential which was presented during Identity Assurance.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	b.	A QAR MUST ask the OOR Person verbally to confirm the AID that was sent in the Legal Entity OOR AUTH vLEI Credential. If the AID provided by the OOR Person does not match the AID sent in the Legal Entity OOR AUTH vLEI Credential, the OOB session ends.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	c.	The QAR MUST use an OOB protocol (such as a QR code or live chat) to share the QVI AID with the OOR Person.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	d.	The OOR Person MUST use an OOB protocol (such as a QR code or live chat) to share its AID with the QAR.	X			X; covered as part of the Credential issuance process with vLEI software

e.	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. The Challenge Message MUST be unique to the OOB session.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
f.	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			X; covered as part of the Credential issuance process with vLEI software
g.	The QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
h.	When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the OOR Person's signature.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
6.3.2 For a Legal Entity with a sole employee					
1. Preparing for authorization of an OOR vLEI Credential by a sole employee (who is at the same time DAR, LAR and OOR Person)					
a.	A credential wallet MUST be set up for the OOR Person.	X			
b.	The LAR as OOR Person MUST generate its AID for an Official Organizational Role vLEI Credential to include in the OOR AUTH vLEI Credential.	X			X; covered as part of the Credential issuance process with vLEI software
c.	Since the OOR Person also is the only LAR, as the sole authorized signer as the LAR MUST issue a Legal Entity OOR AUTH vLEI Credential to the QVI.	X			X; covered as part of the Credential issuance process with vLEI software
i.	The LAR MUST follow the usage rules below for specifying OOR long names in Legal Entity OOR AUTH vLEI Credentials.	X			
1.	The OOR long name MUST be specified in the Legal Entity OOR AUTH vLEI Credential.	X			
2.	If the OOR long name is included in the ISO 5009 Official Organization Role lists, then the long name of the role and its corresponding OOR code MUST be included in the Legal Entity OOR AUTH vLEI Credential. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.	X			
3.	If the OOR long name is specified in public documents, but not in the ISO 5009 Official Organization Role lists, used by the QVI to validate the person in the role, then the role as specified in these documents MUST be included in the Legal Entity OOR AUTH vLEI credential.	X			
4.	If the OOR long name is specified in other documents provided by the Legal Entity, but not in the ISO 5009 Official Organization Role lists, and used by the QVI to validate the person in the role, then the role as specified in these documents MUST be included in the Legal Entity OOR AUTH vLEI credential.	X			
d.	The OOR Person as LAR MUST indicate consent that their name and OOR to be published on the on the LEI page of the Legal Entity on gleif.org when preparing the QVI QUTH OOR vLEI credential.	X			X; Credential format in vLEI software
2. Preparing for issuance of an OOR vLEI Credential by a QVI					
a.	Based on the information contained in the Legal Entity OOR AUTH vLEI Credential received by the QVI:	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
i.	A QAR MUST validate 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 using the GLEIF API.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
ii.	A QAR MUST validate the Legal Entity Identifier (LEI) of the Legal Entity has a LEI Entity Status of Active and a LEI Registration Status of Issued, Pending Transfer or Pending Archival in the Global LEI System using the GLEIF API.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
iii.	A QAR MUST validate the name and the Official Organizational Role of an OOR Person using one or more official public sources. An example of documentation that can be used to validate the name and Official Organizational Role of an OOR Person are a certified copy of documentation accessed directly by the QAR from a business registry.	X		X; requirement in Credential Framework	
iv.	If the OOR long name that the QAR has validated using public sources does not match the OOR long name in the OOR AUTH vLEI Credential, then the QAR MUST inform the LAR.	X		X; requirement in Credential Framework	

	v.	If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the QAR MUST request from the LAR(s) copies of documents of the Legal Entity. Examples of documentation that can be provided by the Legal Entity to validate the name and Official Organizational Role of an OOR Person are a notarized copy of statutes or articles, Board minutes or a certificate of incumbency provided by the Legal Entity. Use of documents not certified or notarized or documents found on websites or through links provided solely by the Legal Entity are not acceptable for this validation.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	vi.	If the name and the Official Organizational Role of the OOR Person cannot be validated using official public sources or copies of documents of the Legal Entity, then the QAR MUST notify the OOR Person as LAR that an OOR vLEI Credential cannot be issued and the OOR Person as LAR MAY authorize instead the issuance of an ECR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b. Identity Verification by a QAR					
	i.	Identity Verification (Assurance and Authentication) of a person serving in an OOR Person by its QVI MUST be performed prior to approval by a QAR of the issuance of an OOR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	iii. Identity Authentication of the OOR Person by a QAR	The following steps MUST be performed in this order during a continuous web meeting OOBI session.				
	a.	A QAR MUST perform manual verification of the OOR Person's legal identity in the identity credential which was presented during Identity Assurance.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	b.	A QAR MUST ask the OOR Person verbally to confirm the AID that was sent in the Legal Entity OOR AUTH vLEI Credential. If the AID provided by the OOR Person does not match the AID sent in the Legal Entity OOR AUTH vLEI Credential, the OOBI session ends.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	c.	The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the OOR Person.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	d.	The OOR Person MUST use an OOBI protocol (such as a QR code or live chat) to share its AID with the QAR.	X			X; covered as part of the Credential issuance process with vLEI software
	e.	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. The Challenge Message MUST be unique to the OOBI session.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	f.	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			X; covered as part of the Credential issuance process with vLEI software
	g.	The QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	h.	When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the OOR Person's signature.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	i.	A Challenge Message MAY be sent from the OOR Person to the QAR, signed and returned by the QAR to the OOR Person and the QAR's signature verified by the OOR Person.	X			
6.4 Issuance	1.	The Legal Entity validation and OOR Person Identity Verification process outlined in section 6.3 MUST be completed before OOR vLEI Credential issuance can begin.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	2.	The QAR MUST follow the usage rules specified below for OOR long names, OOR codes, OOR abbreviations and Latin Transliteration of OOR long names included in OOR vLEI Credentials. The usage rules followed by LARs for preparing the OOR AUTH vLEI Credential are specified in section 6.3. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	a. Usage rules for QARs for OOR long names and OOR codes, if applicable		X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	If the OOR long name and code, if applicable, specified in the OOR AUTH vLEI Credential does not match either the OOR long name and code specified in the ISO 5009 Official Organization Role lists or the OOR long name in the documents provided by the Legal Entity, then the QAR MUST inform the LAR.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	Usage rules for QARs for abbreviations of OOR roles	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	If an OOR abbreviation exists for an OOR role:	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	1.	If an OOR abbreviation is included in the ISO 5009 Official Organization Role lists for the corresponding OOR role, then the abbreviation listed MUST be included in the OOR vLEI credential. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	

	2.	If the OOR abbreviation is specified in other documents used by the QVI to validate the person in the role, then the abbreviation as specified in these documents MUST be included in the OOR vLEI credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	c.	Usage rule for QARs for the Latin Transliteration of OOR long names	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	For all OORs included in the ISO 5009 Official Organization Role lists, the standard requires long names of OORs in non-Latin character sets to be transliterated into Latin characters. If a Latin transliteration exists for an OOR long name in the ISO 5009 lists, the Latin transliteration MUST appear in the OOR vLEI Credential. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	3.	A workflow MUST be implemented in the operations of the QVI which requires two QARs to be involved in the issuance and signing an OOR vLEI Credential. The first QAR will perform the required above-mentioned Identity Authentication and out-of-band validations and then signs the credential. Another QAR then approves the issuance and signs the OOR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	4.	A QAR MUST send the issued OOR vLEI Credential to the OOR Person who MUST sign the Admit message to accept the credential	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	5.	The QAR then MUST confirm that the OOR Person has Fully Signed the Admit message for the OOR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	6.	A QAR MUST call the vLEI Reporting API with each issuance event of OOR vLEI Credentials.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	7.	GLEIF MUST update the list of vLEI Credentials on the LEI page of the Legal Entity to reflect OOR vLEI credential issuances that have been reported by QVIs.	X		X; assessment and demonstration of GLEIF compliance	
6.5 Revocation	1.	To revoke an OOR vLEI Credential:				
	a.	The Legal Entity MUST revoke OOR vLEI Credentials if the OOR Person no longer holds the OOR specified in the OOR vLEI Credential, either as a result of changing roles or termination of employment, or if the OOR Person rescinds consent for their name and OOR to be published on the LEI page of the Legal Entity on gleif.org.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	To revoke a previously issued OOR vLEI Credential, the LAR(s) MUST revoke the QVI AUTH OOR vLEI Credential related to a specific issuance of an OOR vLEI Credential.	X			X; covered as part of the Credential revocation process with vLEI software
	c.	The QAR then MUST revoke the OOR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with vLEI software
	d.	A QAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	e.	A QAR MUST call the OOR Reporting API with each revocation event of Legal Entity Official Organizational Role vLEI Credentials.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	f.	GLEIF MUST remove the details of the OOR vLEI Credential that have been published on the LEI page of the Legal Entity on gleif.org when notified through the vLEI Reporting API about the revocation of an OOR vLEI Credential.	X		X; assessment and demonstration of GLEIF compliance	
	3.	If the QVI has been terminated:				
	a.	b.Validators MUST treat as invalid any OOR vLEI Credentials once the Grace Period has expired. The expiration date of the Grace Period is 90 days after the revocation date of the QVI credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with vLEI software
6.7 Monitoring	1.	GLEIF MUST monitor the QVI Transaction Event Logs (TEs) to detect the issuance of OOR vLEI Credentials which were not reported using the vLEI Reporting API.	X		X; assessment and demonstration of GLEIF compliance	
9.1 Schema	1.	The OOR vLEI Credential MUST be an Authentic Chained Data Container (ACDC) that MUST use for its schema at the time of issuance, the JSON Schema found in: https://github.com/GLEIF-IT/vLEI-schema/blob/main/legal-entity-official-organizational-role-vLEI-credential.json	X			X; Credential format in vLEI software
	2.	The field values in the credential MUST be as follows:				
	a.	The "LEI" field value MUST be the LEI of Legal Entity Holder.	X			X; Credential format in vLEI software
	b.	The "personLegalName" field value MUST be the Legal Name of the Person in the Official Role at the Legal Entity as it appears in the identity credential provided by the OOR Person for Identity Assurance.	X			X; Credential format in vLEI software
	c.	The "officialRole" field value MUST be the Official Organizational Role itself.	X			X; Credential format in vLEI software
	3.	The Sources section of the OOR vLEI Credential MUST contain a source reference to the QVI AUTH vLEI Credential (via SAID) that the issuing QVI received authorizing the issuance of this OOR vLEI Credential. The Sources section of that QVI AUTH vLEI Credential MUST contain a source reference to the Legal Entity vLEI Credential that was issued by the QVI to the Legal Entity and contain the same value for the "LEI" field as the Legal Entity vLEI Credential.	X			X; Credential format in vLEI Software



Spreadsheet Version Date: March 25, 2026 Refer to Change History for Legal Entity Engagement Context Role vLEI (ECR vLEI Credential) Credential Framework in DID URL Change History Tab

Status: Final

Section	Sub-section	"MUST" Statements Legal Entity Engagement Context Role vLEI (ECR vLEI Credential) Credential 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 vLEI Software
6 Issuer Policies						
6.1 Qualifications		The Issuer MUST:				
	1.	be a QVI with which a Legal Entity holding a valid Legal Entity vLEI Credential has contracted with for the issuance of ECR vLEI Credentials, offered by QVIs as a value-added service, or	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	2.	be a Legal Entity holding a valid Legal Entity vLEI Credential who will issue ECR vLEI Credentials directly to ECR Persons.	X			
		The Issuer MUST:	X			
6.2 Credential	1.	use the ECR vLEI Credential schema elements defined in section 9.1. Additional schema elements may be added depending on the requirement of a use case.	X			X; Credential format in vLEI software
	2.	include the Claims marked as Required in section 9.1.	X			X; Credential format in vLEI software
	3.	The LARs of the Legal Entity MUST act as the Issuer of ECR vLEI Credentials when these credentials are issued directly by a Legal Entity.	X			
6.3 Engagement Contact Role (ECR) Person Identity Verification						
	1.	Identity Verification (Assurance and Authentication) of a person serving in an Engagement Context Role (ECR Person) MUST be performed prior to authorization by a LAR of the issuance and prior to the approval by a QAR or a LAR of the issuance of an ECR vLEI Credential. Identity Verification is a necessary process to ensure that digital identities have been verified in a secure manner to prevent impersonation, identity fraud, and ultimately, unauthorized access or use of a vLEI credential.	X			
	a.	Identity Assurance and Identity Authentication MUST be performed using a real-time Out-of-Band-Introduction (OOBI) session. An example is a continuous web meeting attended by all parties on both audio and video in which a QAR and the ECR Person or a LAR and the ECR Person are present.	X			
	b.	If a continuous web meeting is used for the OOBI session: i. Video filters and avatars MUST not be used during the OOBI session. ii. Passcodes and passwords MUST not be displayed on screen (shared) during the OOBI session.	X			
	d. Identity Assurance of an ECR Person					
	i. c.	Proper security access controls MUST be put in place between the QVI and the third-party provider so that the QAR can view the results of identity assurance and confirm that the persons that the third party has conducted identity assurance according to the requirements of the vLEI Ecosystem Governance Framework.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	6.3.1. For issuance by a QVI for a Legal Entity with more than one authorized signer or employee					

	1. Preparing for authorization of an ECR vLEI Credential by a LAR					
	1. Identity Verification (Assurance and Authentication) of an ECR Person by a LAR					
	a. i.	A credential wallet MUST be set up for the ECR Person.	X			
	b. i.	Identity Assurance of a person serving in an Engagement Context Role (ECR Person) MUST be performed prior to authorization of the issuance of an ECR vLEI Credential if the identity of a colleague and other representative of their organizations is not well known in their role in the organization to at least one of the LARs.	X			
	c.	If Identity Assurance is performed, Identity Assurance MUST be completed prior to Identity Authentication.	X			
	d.	Identity Authentication always MUST be performed.	X			
	e.	The LAR MUST request the ECR Person to generate its AID.	X			X; covered as part of the Credential issuance process with vLEI software
	f. Identity Authentication of an ECR Person by a LAR	Then the following steps MUST be performed in this order and completed during a continuous web meeting OOB session.				
	i.	The LAR MUST perform manual verification of the of the ECR Person's legal identity which was presenting during Identity Assurance.	X			X; covered as part of the Credential issuance process with vLEI software
	ii.	The LAR MUST use an OOB protocol (such as a QR code or live chat) to share the Legal Entity AID with the ECR Person.	X			X; covered as part of the Credential issuance process with vLEI software
	iii.	The ECR Person MUST use an OOB protocol (such as a QR code or live chat) to share its AID with the LAR.	X			X; covered as part of the Credential issuance process with vLEI software
	iv.	The LAR 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 OOB session.	X			X; covered as part of the Credential issuance process with vLEI software
	v.	The ECR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the ECR Person MUST acknowledge that this action has been completed.	X			X; covered as part of the Credential issuance process with vLEI software
	vi.	The LAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.	X			X; covered as part of the Credential issuance process with vLEI software
	vii.	When the response to the Challenge Message has been received by the LAR, the LAR MUST verify the ECR Person's signature.	X			X; covered as part of the Credential issuance process with vLEI software

	g. Preparation of the ECR AUTH vLEI Credential by the LARs					
	i.	The LARs MUST create an ECR AUTH vLEI Credential to be presented to the QVI as required in the Authorization vLEI Credential Framework.	X			X; covered as part of the Credential issuance process with vLEI software
	2.Preparing for issuance of an ECR vLEI Credential by a QVI					
	a.	Based on the information contained in the OOR AUTH vLEI Credential received by the QVI:				
	i.	A QAR MUST validate 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 using the GLEIF API.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	A QAR MUST validate the Legal Entity Identifier (LEI) of the Legal Entity has a LEI Entity Status of Active and a LEI Registration Status of Issued, Pending Transfer or Pending Archival in the Global LEI System using the GLEIF API.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b. Identity Verification of an ECR Person by a QVI					
	i.	Identity Verification (Assurance and Authentication) of an ECR Person by its QVI MUST be performed prior to approval by a QAR of the issuance of an ECR vLEI Credential after the receipt of an ECR AUTH vLEI Credential by a QVI.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	Identity Assurance MUST be completed prior to Identity Authentication.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iii. Identity Authentication of an ECR Person by a QVI	Then the following steps MUST be performed in this order and completed during a continuous web meeting OOB session.				
	a.	A QAR MUST perform manual verification of the ECR Person's legal identity which was presented during Identity Assurance.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	A QAR MUST ask the ECR Person verbally to confirm the AID that was sent in the ECR AUTH vLEI Credential. If the AID provided by the ECR Person does not match the AID sent in the ECR AUTH vLEI Credential, the OOB session ends.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	c.	The QAR MUST use an OOB protocol (such as a QR code or live chat) to share the QVI AID with the ECR Person.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	d.	The ECR Person MUST use an OOB protocol (such as a QR code or live chat) to share its AID with the LAR.	X			X; covered as part of the Credential issuance process with vLEI software

	e.	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 AID. The Challenge Message MUST be unique to the OOB session.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	f.	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		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	g.	The QAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	h.	When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the ECR Person's signature.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	6.3.2 For issuance by a QVI for a Legal Entity with a sole authorized signer or employee					
	1. Preparing for authorization of an ECR vLEI Credential by a sole employee (who is at the same time DAR, LAR and ECR Person)					
	a.	A credential wallet MUST be set up for the ECR Person.	X			
	b.	The LAR as ECR Person MUST generate its AID for an Engagement Context Role vLEI Credential to include in the ECR AUTH vLEI Credential.	X			X; covered as part of the Credential issuance process with vLEI software
	c.	Since the ECR Person also is the only LAR, the sole authorized signer or employee as the LAR MUST issue an ECR AUTH vLEI Credential to the QVI.	X			X; covered as part of the Credential issuance process with vLEI software
	2. Preparing for issuance of an ECR vLEI Credential by a QVI					
	a.	Identity Verification (Assurance and Authentication) of an ECR Person by its QVI MUST be performed prior to approval by a QAR of the issuance of an ECR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	c. Identity Authentication of an ECR Person by a QAR	Then the following steps MUST be performed in this order and completed during a continuous web meeting OOB session.				
	i.	A QAR MUST perform manual verification of the ECR Person's legal identity in the identity credential which was presented during Identity Assurance.			X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	A QAR MUST ask the ECR Person verbally to confirm the AID that was sent in the ECR AUTH vLEI Credential. If the AID provided by the ECR Person does not match the AID sent in the ECR AUTH vLEI Credential, the OOB session ends.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iii.	The QAR MUST use an OOB protocol (such as a QR code or live chat) to share the QVI AID with the ECR Person.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iv.	The ECR Person MUST use an OOB protocol (such as a QR code or live chat) to share its AID with the QAR.	X			
	v.	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 AID. The Challenge Message MUST be unique to the OOB session.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	vi.	The ECR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the ECR Person MUST acknowledge that this action has been completed	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	vii.	The QAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	viii.	When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the ECR Person's signature.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software

	6.3.3 For issuance by a Legal Entity with more than one authorized signer or employee					
	1. Preparing for authorization of an ECR vLEI Credential by a LAR					
	a. Identity Verification (Assurance and Authentication) of an ECR Person by a LAR					
	i.	A credential wallet MUST be set up for the ECR Person.	X			
	b.i.	a. Identity Verification (Assurance and Authentication) of an ECR Person MUST be performed prior to authorization of the issuance of an ECR vLEI Credential if the identity of a colleague and other representative of their organizations is not well known in their role in the organization to at least one of the LARs.	X			
	c.	If Identity Assurance is performed, Identity Assurance MUST be completed prior to Identity Authentication.	X			
	d.	Identity Authentication always MUST be performed.				
	e.	The LAR MUST request the ECR Person to generate its AID.	X			X; covered as part of the Credential issuance process with vLEI software
	f. Identity Authentication of an ECR Person by a LAR	Then the following steps MUST be performed in this order and completed during a continuous web meeting OOB session.				
	i.	The LAR MUST perform manual verification of the ECR Person's legal identity in the identity credential which was presenting during Identity Assurance.	X			
	ii.	The LAR MUST use an OOB protocol (such as a QR code or live chat) to share the Legal Entity AID with the ECR Person.	X			X; covered as part of the Credential issuance process with vLEI software
	iii.	The ECR Person MUST use an OOB protocol (such as a QR code or live chat) to share its AID with the LAR.	X			X; covered as part of the Credential issuance process with vLEI software
	iv.	The LAR 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 OOB session.	X			X; covered as part of the Credential issuance process with vLEI software
	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			X; covered as part of the Credential issuance process with vLEI software
	vi.	The LAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.	X			X; covered as part of the Credential issuance process with vLEI software
	vii.	When the response to the Challenge Message has been received by the LAR, the LAR MUST verify the ECR Person's signature.	X			X; covered as part of the Credential issuance process with vLEI software
	g. Preparation of the ECR AUTH vLEI Credential by the LARs					
	i.	The LAR MUST create an ECR AUTH vLEI Credential as required in the Authorization vLEI Credential Framework.	X			X; covered as part of the Credential issuance process with vLEI software
	ii.	The ECR AUTH vLEI Credential MUST be signed by a threshold satisfying number of LARs using the Legal Entity vLEI Credential.	X			X; covered as part of the Credential issuance process with vLEI software
6.4 Issuance						

	6.4.1 For issuance by a QVI:					
	1.	The Legal Entity validation and ECR Person Identity Verification process outlined in section 6.3 MUST be completed before ECR vLEI Credential issuance can begin.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	2.	A workflow MUST be implemented in the operations of the QVI which requires two QARs to be involved in the issuance and signing an ECR vLEI Credential. The first QAR will perform the required above-mentioned Identity Authentication and out-of-band validations and then signs the credential. Another QAR then approves the issuance and signs the ECR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	3.	A QAR MUST send the issued Legal Entity Engagement Context Role vLEI Credential to the ECR Person who MUST sign the Admit message to accept the credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	4.	The QAR then MUST confirm that the ECR Person has Fully Signed the Admit message for the Legal Entity Engagement Context Role vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	6.4.2 For issuance by a Legal Entity:					
	1.	The ECR Person Identity Verification process outlined in section 6.3 MUST be completed before ECR vLEI Credential issuance can begin.	X			
	2.	A workflow MUST be put in place by the Legal Entity for ECR vLEI Role Credentials to meet the requirement for two LARs to sign the ECR vLEI Role Credentials at issuance for Legal Entities with more than one authorized signer or employee.	X			X; covered as part of the Credential issuance process with vLEI software
	3.	A LAR MUST send the issued Legal Entity Engagement Context Role vLEI Credential to the ECR Person who MUST sign the Admit message to accept the credential.	X			X; covered as part of the Credential issuance process with vLEI software
	4.	The LAR then MUST confirm that the ECR Person has Fully Signed the Admit message for the Legal Entity Engagement Context Role vLEI Credential.	X			X; covered as part of the Credential issuance process with vLEI software
	6.5 Revocation					
	6.5.1. For revocation by a QVI:					
	1.	The Legal Entity MUST notify the QVI to revoke an ECR vLEI Credential.	X			
	2.	To revoke a previously issued ECR vLEI Credential, the LAR(s) MUST revoke the ECR AUTH vLEI Credential related to a specific issuance of an ECR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with vLEI software
	3.	The QAR then MUST revoke the ECR vLEI Credential.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with vLEI software
	4.	The QAR MUST perform the revocation within the timeframe specified in the agreement that has delegated the issuance of ECR vLEI Credentials to one or more QVIs, offered by QVIs as a value-added service.	X		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with vLEI software
	b.	Validators MUST treat as invalid any ECR vLEI Credentials once the Grace Period has expired. The expiration date of the Grace Period is 90 days after the revocation date of the QVI credential.	X			
	9. Credential Definition					
	9.1 Schema					
	1.	The ECR vLEI Credential MUST be an Authentic Chained Data Container (ACDC) that MUST use for its schema at the time of issuance, the JSON Schema found in: https://github.com/GLEIF-IT/vLEI-schema/blob/main/legal-entity-engagement-context-role-vLEI-credential.json	X			X; Credential format in vLEI software
	2.	The field values in the credential MUST be as follows:				
	a.	The "LEI" field value MUST be the LEI of Legal Entity Holder.	X			X; Credential format in vLEI software
	b.	The "personLegalName" field value MUST be the Legal Name of the Person in the Engagement Context Role at the Legal Entity as it appears in the identity credential provided by the OOR Person for Identity Assurance.	X			X; Credential format in vLEI software
	c.	The "engagementContextRole" field value MUST be the Engagement Context Role.	X			X; Credential format in vLEI software
	3.	For an Issuer that is a QVI, the Sources section of the ECR vLEI Credential MUST contain a source reference to the ECR AUTH vLEI Credential (via SAID) that the issuing QVI received authorizing the issuance of this ECR vLEI Credential. The Sources section of that ECR AUTH vLEI Credential MUST contain a source reference to the Legal Entity vLEI Credential that was issued by the QVI to the Legal Entity and contain the same value for the "LEI" field as the Legal Entity vLEI Credential.	X			X; Credential format in vLEI software
	4.	For an Issuer that is a Legal Entity, the Sources section of the ECR vLEI Credential MUST contain a source reference to the Legal Entity vLEI Credential (via SAID) held by the Legal Entity that is issuing this ECR vLEI Credential. The value of the "LEI" field of the Legal Entity vLEI Credential MUST match the value of the "LEI" field in this ECR vLEI Credential.	X			X; Credential format in vLEI software