Document Version Date: 2024-04-10

Status: Final

DID URL for the Trust Assurance Framework:

did:keri:EINmHdSg7iV-UIdkkkKyBIH052blyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2024-04-10_vLEI-EGF-v2.0-Trust-Assurance-Framework_v1.4_final.pdf

Change History:

EGF Version	1.0	
Document Version	1.1	
Date	April 3, 2023	
Description of Changes		
	In Technical KERI Infrastructure, replaced 'Verifiable Data Registries (VDRs)' in section 5.6 with 'GLEIF Witness Network'.	
	In QVI Identifier Credential, corrected 'QVI External AID' to 'GLEIF External AID' in Subsection 6.5.	

EGF Version	1.0	
Document Version	1.2	
Date	August 30, 2023	
Description of Changes		
	In Primary Document, updated GLEIF postal address; updated link to the vLEI Ecosystem Governance Framework on GLEIF website.	
	In QVI Identifier Credential, added section 6.3.3 Addition or Replacement of QARs.	
	In Legal Entity Credential, updated section 6.3 Legal Entity Identification to include Identity Assurance requirements for DARs; requirements for the appointment of LARs	
		and for multi-sig and thresholds for signing of the Legal Entity vLEI Credentrial by LARs; corrected 'AVR' to 'LAR' in section 6.3.2.c.i.; added section 6.4 Addition or Replacement of DARs and LARs.
	In QVI AUTH Credential, corrected '9.1' and '9.2' to '10.1' and '10.2' in section 6.2; updated section 6.3 Identity Verification to refer to the Identity Assurance and Identity Authentication sections in the OOR and ECR vLEI Credential Frameworks;	
		updated section 6.4 Issuance to include requirements for multi-sig and thresholds for issuance of the QVI AUTH vLEI Credentials; updated section 9 Privacy Considerations with the requirement for OOR Person consent;
		updated section 10 Credential Definition to clarify the requirement for the 'personLegalName' field value.
	In OOR Credential, restructured section 6.5 OOR Person Identity Verification to indicate clearly requirements for Legal Entity Authorized Representatives (LARs) and for Qualified vLEI Issuers (QVIs) and to account for Legal Entities with a sole employee;	
		moved requirement for LARs to issue the Legal Entity OOR Authorization vLEI Credential from section 6.6.2 to section 6.5.1.i.; updated section 9 Credential Definition to clarify the requirement for the 'personLegalName' field value.
	In Engagement Context Credential, Clearly indicated 'or' for requirements in section 6.1; updated the '10.1' and '10.2' to '9.1' and '9.2' in section 6.2;	
		clarified section headings in sections 6.3, 6.4, 6.5 (Legal Entity, Legal Entity Authorized Representative (LAR) and ECR Person Identity Verification) and 6.6 to indicate requirements for issuance by a QVI and issuance by a Legal Entity;

EGF Version	2.0	
Document Version	1.3	
Date	December 15, 2023	
Description of Changes		
	In Information Trust Policies, clarification added regarding includes International or trans-national governance authorities or standards organizations in section 3, Regulatory Compliance.	
	In Technical KERI Infrastructure, Updated link to KERI specification in section 1.1; clarification in section 5.6 GLEIF Witness Network that GLEIF must set up and maintain its own Witness pool; formatting, editing (for example, consistent capitalization of defined terms).	
	In Technical vLEI Credentials, updated link to specifications in section 1.1; updated list of requirements for vLEI ACDCs in section 3, Requirements for vLEI ACDCs;eliminated the reference to the SIS specification in section 4, vLEI Credential Schema;	
		updated inclusion of the Public Transaction Event Log (PTEL) within the Authentic Chained Data Container (ACDC) specification in section 6.6, Credential Issuance and Revocation Registry Requirements; formatting, editing (for example, consistent capitalization of defined terms).
	In Technical CredentialSchemaReg, updated link to specifications in Related Specifications section 1.1; updated URLs in Schema Table, section 2.3, to GLEIF-IT hosted URLs; formatting, editing (for example, consistent capitalization of defined terms).	
	In QVI Identifier Credential, added Note that the QVI DAR also may be designated as a QAR in section 6.3.1.;updated section 6.3.2. QVI Identity Authentication to clarify that the QARs are part of the QVI multi-sig group;	
		updated specification references and links in sections 10.1 Schema; corrected reference to QVI vLEI Credential in section 10.1.1.
	In Legal Entity Credential, added to section 6.3 examples of acceptable documentation that QARs, or Third-Party Service providers, can use in the Identity Assurance of DARs;Added Note that a DAR also can be a LAR in section 6.3.1.f.;	
		clarified the presentation of Legal Entity vLEI Credentials by LARs in section 6.3.1.f.; corrected reference to Legal Entity vLEI Credential in section 6.4.4.;
		added section 6.7, Monitoring, for the issuance of Legal Entity vLEI Credentials; updated GLEIF-IT hosted link for schema in section 9.1.1. Schema; updated references to specification references and links in section 9.1.3., Schema;
		added credential usage paragraph in section 9.1.4., Schema.
	In QVI AUTH vLEI Credential, updated 'and' to 'or' in initial sentence in section 6.3 Identity Verification;added frequency of GLEIF checking TEL in section 6.7;	
		updated specification references and links in section 9 Privacy Considerations and in sections 10.1 and 10.2 Schema; updated GLEIF-IT hosted link to schema in sections 10.1 and 10.2 Schema.
	In OOR Credential, added the usage rules that the LAR must follow for specifying OOR roles in Legal Entity OOR AUTH vLEI Credentials in section 6.5.1.j. and 6.5.2.c. OOR Person Identity Verification;	
		updated sections 6.5.1.2. and 6.1.2.2., OOR Person Identity Verification, with examples of acceptable documentation that can be used by QARs to validate the name and Official Organizational Role of an OOR Person;
		deleted repeated 'on the' in section 6.5.5.1.f. OOR Person Identity Verification; added the usage rules that a QAR must follow for Official Organizational Role Codes and Reference Data included in OOR vLEI Credentials in section 6.6, Issuance;
		updated GLEIF-IT hosted link to schema in section 9.1.1., Schema; updated inclusion of Issuance and Presentation (IPEX) protocol within the Authentic Chained Data Container (ACDC) specification in section 9.1.3., Schema.
		added credential usage paragraph in section 9.1.5., Schema.
	In Engagement Context Credential, updated specification references and links in section 7.2 Privacy Considerations; updated GLEIF-IT hosted link to schema in section 9.1.1., Schema;	
		updated inclusion of Issuance and Presentation (IPEX) protocol within the Authentic Chained Data Container (ACDC) specification in section 9.1.4, Schema;
		added credential usage paragraph in section 9.1.5., Schema.

EGF Version	2.0	
Document Version	1.4	
Date	April 10, 2024	
Description of Changes		
	In QVI Identifier Credential, clarified that credential wallets are to be set up for the QVi Authorized Representatives (QARs) in section 6.3.2.a., QVI Identity Verification;	
		added requirement not to use video filters and avatars during OOBI sessions in section 6.3.2.d., QVI Identity Verification, section 6.4.2.a, Creation of QVI Delegated AIDs, and section 6.5.2, Delegation of QVI Delegated AIDs;
		eliminated the duplicate steps in section 6.4.2.a, Creation of QVI Delegated AIDs;
		corrected reference of 'External QAR' to 'External GAR' in section 6.7, QVI vLEI Credential Revocation.
	In Legal Entity Credential, clarified signing requirements for the Legal Entity vLEI Credential in section 6.3.1.f.iv., Legal Entity Identity Verification;	
		clarified credential wallet set up in section 6.3.3.a., Legal Entity Identity Verification;
		added requirement not to use video filters and avatars during OOBI sessions in section 6.3.3.c., Legal Entity Identity Verification;
		corrected omission of step for creation of the Legal Entity Autonomic Identifier (AID) in section 6.3.3.d.iii., Legal Entity Identity Verification.
	In OOR Credential, added requirement not to use video filters and avatars during OOBI sessions in sections 6.5.1.1.i., 6.5.1.2.b.ii., and 6.5.2.2.b.ii., OOR Person Identity Verification;	
		corrected omission of the step of the sharing of the Legal Entity Autonomic Identifier (AID) in section 6.5.1.1.i.i., OOR Person Identity Verification;
		corrected omission of the step of the sharing of the QVI Autonomic Identifier (AID) in sections 6.5.1.2.c.i. and 6.5.2.2.c.i.,OOR Person Identity Verification.
	In Engagement Context Credential, added requirement not to use video filters and avatars during OOBI sessions in sections 6.5.1.1.h., 6.5.1.2.a.ii., 6.5.2.2.b., 6.5.2.2.f.ii., 6.5.3.2.c.and ECR Person Identity Verification;	
		corrected omission of the step of the sharing of the Legal Entity Autonomic Identifier (AID) in section 6.5.1.1.h.i., ECR Person Identity Verification;
		corrected omission of the step of the sharing of the QVI Autonomic Identifier (AID) in sections 6.5.1.2.b.i. and 6.5.2.2.f.iii.,,ECR Person Identity Verification.

verifiable LEI (vLEI) Ecosystem Governance Framework v2.0 Trust Assurance Framework — Document Version 1.4 final — 2024-04-10

Spreadsheet Version Date: 2023-08-30 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; compliant to Documented Information Procedure		
	4.a.	All revisions to Controlled Documents MUST be identified with a revision number that is a sequential integer.		X; Document approvals follow the defined Documented Information Procedure		
	5.	All revisions to the vLEI Ecosystem Governance Framework MUST be approved by GLEIF using its Change Management Process.		X; Document approvals follow the defined Documented Information Procedure		

verifiable LEI (vLEI) Ecosystem Governance Framework v2.0 Trust Assurance Framework — Document Version 1.4 final — 2024-04-10

Spreadsheet Version Date: 2023-12-15 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. This plan MUST include procedures and forms that GLEIF and the Qualified vLEI Issuers use responsively to communicate security events and their disposition.			X; appropriate response plan provided to GLEIF during vLEI Issuer Qualification and confirmed during Annual vLEI Issuer Qualification; existence of forms communicating security events and their disposition	
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.	GLEIF MUST provide technical changes/upgrades to the vLEI software to Qualified vLEI Issuers.		X; audit of GLEIF compliance		
	2.	Qualified vLEI Issuers MUST successfully install, test and implement the GLEIF-supplied vLEI software within stated timeframes.			X; software working by stated timeframes	

verifiable LEI (vLEI) Ecosystem Governance Framework v2.0 Trust Assurance Framework **Document Version 1.4 final** **2024-04-10**

Spreadsheet Version Date: 2022-12-16

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.	There MUST be availability targets defined for all vLEI services included in Appendix 5 of the vLEI Issuer Qualification Agreement, Qualified vLEI Issuer Service Level Agreement (SLA).	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	

verifiable LEI (vLEI) Ecosystem Governance Framework v2.0 Trust Assurance Framework — Document Version 1.4 final — 2024-04-10

Spreadsheet Version Date: 2023-12-15 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. Endorser (Backer) Management						
2.1 Witness Pool:		A Witness Pool:				
	1.	MUST use KERI Agreement Algorithm for Control Establishment (KAACE) sufficient majority threshold on a minimum pool of 5 Witnesses.	X		X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
	3.	MUST publish Witnesses to at least one ecosystem discovery mechanism:	X		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 OOBI (out-of-band-introduction) to witness or witnesses	X		X; assessment and demonstration of compliance	
	b.	Publish OOBIs for witnesses on web site(s) discoverable by search engines.	X			
	c.	KERI Distributed Hash Table (DHT)	X		X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
	d.	DID method resolvers	X		X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
	e.	Ledgers	X		X; assessment and demonstration of compliance	
2.2 Registrar (Ledger):		A Registrar (Ledger):				
	1.	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; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
	b.	A DID method MUST be approved down to the ledger-specific level	X		X; assessment and demonstration of compliance	X; covered by KERI Key Management Architecture
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	4.1.1 Strength	All key-pairs MUST be generated using a cryptographic algorithm with at least 128 bits of cryptographic strength. This includes using a source of entropy of at least 128 bits of cryptographic strength for the salt or seed used to generate the private key of the key pair.	X			X; covered by KERI Key Management Architecture
	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.	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; confirmation during Annual vLEI Issuer Qualification	
	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		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
4.3 Signature Verification Infrastructure	1.	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		X; confirmation during Annual vLEI Issuer Qualification	
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 Notaries as witnesses.	X		X; assessment and demonstration of GLEIF compliance	
	2.	The OOBI 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		X; assessment and demonstration of GLEIF compliance	
	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		X; assessment and demonstration of GLEIF compliance	
	i.	Qualified vLEI Issuers	X		X; confirmation during Annual vLEI Issuer Qualification	
	c.	MUST be stored as a file on a public GLEIF GitHub repository.	X		X; assessment and demonstration of GLEIF compliance	
	d.	MUST be shared on the following social media:	X		X; assessment and demonstration of GLEIF compliance	
	i.	LinkedIn and Twitter				
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			
	2.	The GLEIF Root AID MUST be a threshold multi-sig with weighting requirements that have been determined by GLEIF.	X			X; covered by KERI Key Management Architecture
	3.	Key Pair Creation and Storage Infrastructure MUST be within a TEE.	X			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; 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 KAACE.	X			X; covered by KERI Key Management Architecture
	2.	The number of Witnesses on any single web host provider MUST be less than the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)	X			X; covered by KERI Key Management Architecture
	3.	The number of Witnesses on any single continent MUST be less than the sufficient threshold as per KAACE.	X			X; covered by KERI Key Management Architecture
	4.	The number of Witnesses in any single political jurisdiction MUST be less than the sufficient threshold as per KAACE.	X			X; covered by KERI Key Management Architecture
	6.	The secrets in the key store MUST be encrypted with the key loaded dynamically whenever the Witness service is started.	X			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; covered by KERI Key Management Architecture
5.5 GLEIF External Delegate AID	1.	GLEIF MUST set the Do Not Delegate configuration property on Qualified vLEI Issuer AIDs. NOTE: This may change in the future to enable horizontal scalability.	X			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; covered by KERI Key Management Architecture
5.7 GLEIF Watcher Network	2.	Larger pool sizes MUST use KAACE sufficient majority thresholds.	X			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; covered by KERI Key Management Architecture
	5.	When used, the encryption key store MUST reside on a different device or host from that of the Watcher service.	X			X; covered by KERI Key Management Architecture
5.8 GLEIF Key Management	1.	The specifc holders of cryptographic keys MUST be kept confidential and shall be determined by GLEIF internal policy.	X		X; assessment and demonstration of GLEIF compliance	
	3.	Signing keys MUST be rotated whenever there is a likelihood of key compromise.	X			X; covered by KERI Key Management Architecture
	4.	The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.	X		X; assessment and demonstration of GLEIF compliance	
	6.	GLEIF policies for approving rotation of the issuing keys for the GLEIF-Delegated issuing identifier:	X			X; covered by KERI Key Management Architecture
	a.	MUST use an OOB (out-of-band) MFA (multi-factor authorization) mechanism to approve Delegated AID rotation.	X		X; assessment and demonstration of GLEIF compliance	
6. Qualified vLEI Issuer KERI Profile						
6.2 Delegated AIDs	1.	For added security, Qualified vLEI Issuers:				
	a.	MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
	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 Qualified vLEI Issuer Endorser Support: Witness Pool or Ledger Registrar	1.	An Endorser MUST use either a Witness Pool or a Ledger Registrar for Endorsement	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
6.3.1 Witness Pool	1.	The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAACE.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
	2.	The Witness Signing Key Pair key store MAY reside on the Witness Service host but MUST use dedicated user only permissions on the key store directory and its contents.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
	4.	The encryption key store MUST reside on a different device or host from that of the Witness service.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture

6.3.2 Ledger Registrar	1.	Registrar Signing Key Pair key store MAY reside on the Registrar Service host but MUST use dedicated user only permissions on the key store directory and its contents.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
	3.	The encryption key store MUST reside on a different device or host from that of the Registrar service.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
6.4 Watchers	2.	Larger pool sizes MUST use KAACE sufficient majority thresholds.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
	3.	Watcher Signing Key Pair key store MAY reside on the Watcher Service host but MUST use dedicated user only permissions on the key store directory and its contents.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
	5.	When used, the encryption key store MUST reside on a different device or host from that of the Witness service.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
6.5 Key Management	1.	The specific holders of cryptographic keys MUST be kept confidential and shall be determined by Qualified vLEI Issuer internal policy.	X		X; confirmation during Annual vLEI Issuer Qualification	
	3.	GLEIF External GARs (GLEIF Authorized Representatives) MUST approve a QVI Rotation Event that occurs no less than six months from the last QVI Rotation Event.	X		X; confirmation during Annual vLEI Issuer Qualification	
	4.	Qualified vLEI Issuer Authorized Representatives (QARs) MUST contact GLEIF External GARs for approval of any QVI Rotation Event that occurs less than six months from the last QVI Rotation Event.	X		X; confirmation during Annual vLEI Issuer Qualification	
	5.	Signing keys MUST be rotated whenever there is a likelihood of key compromise.	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
	6.	The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.	X		X; confirmation during Annual vLEI Issuer Qualification	
	7.	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; confirmation during Annual vLEI Issuer Qualification	
6.6 Delegation		The Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to True. (NOTE: This may change in future versions in order to accommodate horizontal scalability of the vLEI signing infrastructure.)	X		X; confirmation during Annual vLEI Issuer Qualification	X; covered by KERI Key Management Architecture
6.7 Key Compromise Monitoring	1.	Qualified vLEI Issuers MUST monitor their public Witnesses for their vLEI issuance and revocation registry for erroneous or malicious issuances and revocations (primarily issuances) in order to in-form their key management process that a key recovery may be required.	X		X; confirmation during Annual vLEI Issuer Qualification	
6.8 Key Compromise Recovery	1.	In any case of key compromise, a Qualified vLEI Issuer MUST:				
	a.	Report to GLEIF all key compromise recovery operations within 24 hours of gaining knowledge of the key compromise.	X		X; confirmation during Annual vLEI Issuer Qualification	
	b.	Investigate as expeditiously as possible at its own expense the source of the key compromise and make a full report of the investigation to GLEIF.	X		X; confirmation during Annual vLEI Issuer Qualification	
	c.	Make a recovery Rotation Event that forks their KEL and submit the recovering Rotation Event and signatures to GLEIF in order that GLEIF may anchor a confirmation seal in its KEL.	X		X; confirmation during Annual vLEI Issuer Qualification	
	d.	Send a key recovery event explanation to GLEIF for publication in GLEIF's public registry of Qualified vLEI Issuer recovery events.	X		X; confirmation during Annual vLEI Issuer Qualification	
6.9 vLEI Issuance and Revocation Policies	1.	Qualified vLEI Issuers MUST monitor their public Witnesses for their vLEI issuance and revocation registry for erroneous or malicious issuances and revocations (primarily issuances) in order to in-form their key management process that a key recovery may be required.	X		X; confirmation during Annual vLEI Issuer Qualification	
6.10 Challenge Message Policies	1.	The Challenge Message MUST include a cryptographic nonce generated in real time.	X			X; covered by KERI operations
	3.	The Challenge Response Message MUST be Fully Signed by the Responder.	X			X; covered by KERI Key Management Architecture
	4.	The Challenger MUST verify that:				
	a.	The Fully Signed Response contains the same cryptographic nonce as the Challenge Message.	X			X; covered by KERI Key Management Architecture
	b.	The signatures of the Responders were generated by the private keys that control the Responder's AID.	X			X; covered by KERI Key Management Architecture
6.11 Policies for Sharing Authenticated AIDs	1.	Contact sharing with new members of a group multi-sig AID MUST be performed by a threshold satisfying number of existing members.	X			X; covered by KERI operations
	2.	New members MUST be able to Spot Check through Identity Authentication and the Challenge Response process any new authenticated AID they receive from existing members or their new group multi-sig AID.	X			X; covered by KERI Key Management Architecture

verifiable LEI (vLEI) Ecosystem Governance Framework v2.0 Trust Assurance Framework — Document Version 1.4 — 2024-04-10

Spreadsheet Version Date: 2023-12-15 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 that use the did:keri Method.				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 for ACDC and KERI.	X			X; covered as part of vLEI software

Spreadsheet Version Date: 2023-12-15 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 OOBI 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 OOBI 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 OOBI 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 OOBIs 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 OOBI 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 OOBI 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 OOBIs 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 OOBI 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 satisficing 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 satisficing 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

verifiable LEI (vLEI) Ecosystem Governance Framework v2.0 Trust Assurance Framework — Document Version 1.4 final — 2024-04-10

Spreadsheet Version Date: 2024-04-10 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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; Credential format in vLEI software
6.3 QVI Identity Verification	1. Identity Assurance					
	a.	An External GLEIF Authorized Representative (External GAR) MUST perform identity assurance of a person serving in the role of QVI Authorized Representative (QAR) to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html).	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for GLEIF	
	b.	A minimum of two QARs MUST form the QVI multi-sig group.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	c.	An External GAR MUST lead for the anchoring action for the QVI External Delegated AID described below.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer	
	b.	The QARs that formed the QVI multi-sig group MUST participate in the Identity Authentication.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer	
	c.	An External GAR and the QAR MUST establish a real-time OOBI session in which the External GAR and the QAR are present. An example is a continuous web meeting attended by all parties on both audio and video.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
	e.	The following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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 the QAR's legal identity for which the External GAR has already performed Identity Assurance. An example is the QAR visually presenting one or more legal identity credentials and the External GAR compares the credentials verified during Identity Assurance to the QAR Person.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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 OOBI protocol (such as a QR code or live chat) to share the GLEIF External Delegated AID (GEDA) with the QAR.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with vLEI software
	iii.	An QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the External GAR.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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 OOBI session.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for GLEIF	X; covered as part of the Credential issuance process with vLEI software
	v.	The QAR MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the QAR MUST acknowledge that this action has been completed.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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 the QAR.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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 the QAR.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework			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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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 OOBI session for a given QVI Delegated AID.				
	a.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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 Delegated AID GLEIF Authorized Representative (External GARs) as the External Delegated AID GLEIF Authorized Representative (External GAR Lead).	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	
	a.	The QAR Lead initiates a set of QARs to create a multi-sig group and the QARs mutually are authenticated.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	b.	The QAR Lead initiates the creation of the Inception Event using the published GLEIF External AID as the Delegator.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer	X; covered as part of the Credential issuance process with vLEI software
	c.	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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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 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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		X; assessment and demonstration of compliance for Qualified vLEI Issuer and GLEIF	X; covered as part of the Credential issuance process with vLEI software
	e.	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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework		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; requirement in the Identifier Governance Framwork and vLEI Credential Framework			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; requirement in the Identifier Governance Framwork and vLEI Credential Framework			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; requirement in the Identifier Governance Framwork and vLEI Credential Framework			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; requirement in the Identifier Governance Framwork and vLEI Credential Framework			X; Credential format in vLEI software
	2.	The field values in the credential MUST be as follows:	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework			X; Credential format in vLEI software
	a.	The "LEI" field value MUST be the LEI of the QVI.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework			X; Credential format in vLEI software
	b.	The "gracePeriod" field value MUST be at least 90 (ninety) Days.	X; requirement in the Identifier Governance Framwork and vLEI Credential Framework			X; Credential format in vLEI software

verifiable LEI (vLEI) Ecosystem Governance Framework v2.0 Trust Assurance Framework — Document Version 1.4 final — 2024-04-10

Spreadsheet Version Date: 2024-04-10 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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	2.	follow all of the requirements specified in the vLEI Issuer Qualification Agreement.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	3.	use the vLEI software for hosting Witnesses, Watchers and for Key Management.	X; requirement in Credential Framework		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.				
		The Issuer MUST:				
6.2 Credential	1.	use the Legal Entity vLEI Credential schema defined in section 8.1.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in vLEI software
	2.	include the Claims marked as Required in section 8.1.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in vLEI software
6.3 Legal Entity Identity Verification	1. Identity Assurance of the Legal Entity's Designated Authorized Representative (DAR)					
	a.	A QVI Authorized Representative (QAR) MUST perform identity assurance of a person serving in the role of a Legal Entity Designated Authorized Representative (DAR) that will designate the Legal Entity Authorized Representatives (LARs) to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html).	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	As an alternative to a., the QVI MAY use Third-Party Services to perform identity assurance on the DAR.				
	i.	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 to ensure that the third-party provider follows the requirements of the vLEI Ecosystem Governance Framework.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	c.	The QAR MUST verify the signing authority of the DAR. Examples of authorization documentation that can be provided are a certified copy of documentation accessed directly by the QAR from a business registry, or a notarized copy of statutes or 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 as proof of signing authority.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	d.	A QAR MUST verify that the LEI supplied for the Credential by the DAR is the LEI of the Legal Entity for which the issuance request for the Credential has been made.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	e.	A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity has 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 Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	f.	The DAR SHOULD designate at least three (3) LARs if the Legal Entity has 3 or more authorized signers or authorized employees that can be designated for signing credentials in order to use the greater security of KERI multi-sig protocols.	X; requirement in Credential Framework			
	i.	The Legal Entity MAY appoint less than three (3) LARs if less than 3 authorized signers exist or less than 3 employees can be designated for signing credentials on behalf of the Legal Entity.	X; requirement in Credential Framework			
	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	X; requirement in Credential Framework			
	iii.	Only one LAR signature is required for a Legal Entity with a sole employee or authorized signatory.	X; requirement in Credential Framework			
	iv.	he Legal Entity vLEI Credential MUST be multi-signed by a threshold satisfying number of LARs before the credential can be used or presented.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process vLEI software
	2. Identity Assurance of the Legal Entity Authorized Representative(s) (LAR(s))					
	a.	A QAR MUST perform identity assurance of a person serving in the role of a Legal Entity Authorized Representative (LAR) to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html). Even when IAL2 is used for Identity Assurance, a real-time OOBI session is required as specified 6.3.b. (essentially including the IAL3 requirement for a Supervised Remote In-person session).	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	As an alternative to a., the QVI MAY use Third-Party Services to perform identity assurance on the LARs.	X; requirement in Credential Framework			
	i.	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 have been identity assured are the LARs that join the real-time OOBI session specified in 6.3. b.), as well as to ensure that the third-party provider follows the requirements of the vLEI Ecosystem Governance Framework.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	

	3. Identity Authentication					
	a.	A credential wallet MUST be set up for the Legal Entity and for each LAR.	X; requirement in Credential Framework			
	b.	A QAR and the LARs MUST establish a real-time OOBI session in which the QAR and all LARs are present. An example is a continuous web meeting attended by all parties on both audio and video.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	c.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	d.	The following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	The QAR MUST perform manual verification of each LAR's legal identity for which the QAR has already performed Identity Assurance. An example is each LAR visually presenting one or more legal identity credentials and the QAR compares the credentials verified during Identity Assurance to the LAR Person.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI Autonomic Identifier (AID) with the LARs.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process vLEI software
	iii.	A LAR MUST create the Legal Entity AID.	X; requirement in Credential Framework			
	iv.	Each LAR MUST use an OOBI protocol (such as a QR code or live chat) to share the Legal Entity AID with the QAR.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process vLEI software
	v.	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 OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process vLEI software
	vi.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
	vii.	The QAR MUST verify in real time that a response to the Challenge Message was received from each LAR.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process vLEI software
	viii.	When all responses to Challenge Messages sufficient to satisfy the multi-sig threshold have been received, the QAR MUST verify the complete set of signatures.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with KERI
	a.	When new DARs are appointed to replace or add LARs, a QAR MUST perform identity assurance of a person serving in the role of a new DAR as specified in sections 6.3.1a and 6.3.1.b.	X; requirement in Credential Framework			
	b.	When DARs add or replace LARs after the issuance of the Legal Entity vLEI Credential, the steps within 1. Identity Assurance and Identity Authentication MUST be followed, beginning with 6.3.1.e.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with KERI
6.4 Issuance	1.	The Legal Entity Identity Verification process outlined in section 6.3 MUST be completed before Legal Entity vLEI Credential issuance can begin.	X; requirement in Credential Framework			
	2.	In addition, a workflow MUST be implemented in the operations of the QVI which requires, prior to issuing and signing an Legal Entity vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR. Another QAR then approves the issuance and signs the Legal Entity vLEI Credential.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	3.	QVIs MUST call the vLEI Reporting API with each issuance event of Legal Entity vLEI Credentials.	X; requirement in Credential Framework		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 Legal Entity vLEI credential issuances that have been reported by QVIs.	X; requirement in Credential Framework		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; requirement in Credential Framework		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; requirement in Credential Framework		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; requirement in Credential Framework		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; requirement in Credential Framework		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; requirement in Credential Framework		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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
6.7 Monitoring	1.	GLEIF MUST monitor the QVI Transaction Event Logs (TELs) to detect the issuance of Legal Entity vLEI Credentials which were not reported using the vLEI Reporting API.	X; requirement in Credential Framework		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; requirement in Credential Framework			X; Credential format in KERI code
	2.	The field values in the credential MUST be as follows:	X; requirement in Credential Framework			X; Credential format in KERI code
	a.	"LEI" field value MUST be the LEI of Legal Entity Holder.	X; requirement in Credential Framework			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; requirement in Credential Framework			X; Credential format in KERI code

Spreadsheet Version Date: 2023-12-15 Refer to Change History for Qualified vLEI Issuer 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; requirement in Credential Framework			X; covered as part of the Credential issuance process vLEI software
6.2 Credential	1.	The Issuer MUST:				
	1.	use the QVI 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; requirement in Credential Framework			X; Credential format in vLEI software
	2.	include the Claims marked as Required in the schema indicated in 9.1 and 9.2.	X; requirement in Credential Framework			
6.3 Identity Verification		LARs MUST include the Autonomic Identifiers (AIDs) of Official Organizational Role Persons (OOR Persons) or Engagement Context Role Persons (ECR Persons) as an element within the QVI AUTH vLEI Credentials issued for each vLEI Role Credential.	X; requirement in Credential Framework			X; Credential format in vLEI software
	1. Identity Assurance					
	a.	The requirements for Identity Assurance for the issuance of vLEI Role Credentials specified in the preparing for authorization of OOR and ECR vLEI Credentials MUST be followed for the issuance of QVI AUTH vLEI Credentials. For OOR vLEI Credentials, the relevant section in the Credential Framework is 6.5.1.1. For ECR vLEI Credentials, the relevant sections in the Credential Framework are 6.5.1.1., 6.5.2.d. and 6.5.3.1.	X; requirement in Credential Framework			
	2. Identity Authentication					
	a.	The requirements for Identity Authentication for the issuance of vLEI Role Credentials specified in the preparing for authorization of OOR and ECR vLEI Credentials MUST be followed for the issuance of QVI AUTH vLEI Credentials. For OOR vLEI Credentials, the relevant sections in the Credential Framework are 6.5.1.2.b. and 6.5.2.2.b. For ECR vLEI Credentials, the relevant sections in the Credential Framework are 6.5.1.2.a., 6.5.2.2.e. and 6.5.3.2.	X; requirement in Credential Framework			
6.4 Issuance						
	6.4.1 For a Legal Entity with more than one authorized signer or employee					
	1.	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 and ECR Person, as elements within the appropriate QVI AUTH vLEI Credential for the issuance of the associated vLEI Role Credential.	X; requirement in Credential Framework			X; Credential format in vLEI software
	2.	The signatures on the QVI AUTH vLEI Credential MUST match the signing threshold of the AID of the Legal Entity vLEI Credential.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process vLEI software
	4.	A LAR MUST issue QVI AUTH vLEI Credential explicitly authorizing the QARs of a QVI to issue each vLEI Role Credential. The QVI AUTH vLEI Credential will become part of the chain of the vLEI Role Credentials.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process vLEI software
	6.4.2 For a Legal Entity with a sole employee					
	1.	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 and ECR Person, as elements within the appropriate QVI AUTH vLEI Credential for the issuance of the associated vLEI Role Credential.	X; requirement in Credential Framework			X; Credential format in vLEI software

	2.	The signatures on the QVI AUTH vLEI Credential MUST match the signing threshold of the AID of the Legal Entity vLEI Credential, which in this case is a sole signer.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process vLEI software
	3.	A LAR MUST issue QVI AUTH vLEI Credential explicitly authorizing the QARs of a QVI to issue each vLEI Role Credential. The QVI AUTH vLEI Credential will become part of the chain of the vLEI Role Credentials.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process vLEI software
6.5 Revocation	1.	To revoke a previously issued vLEI Role Credential, the LAR(s) MUST revoke the QVI AUTH vLEI Credential related to a specific issuance of a vLEI Role Credential	X; requirement in Credential Framework			X; covered as part of the Credential revocation process with vLEI software
	2.	The QAR then MUST revoke the vLEI Role Credential.	X; requirement in Credential Framework		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 (TELs) 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; requirement in Credential Framework		X; assessment and demonstration of GLEIF compliance	
10 Credential Definition						
10.1 Schema QVI OOR AUTH vLEI Credential	1.	The QVI 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; requirement in Credential Framework			X; Credential format in vLEI software
	2.	The field values in the credential MUST be as follows:	X; requirement in Credential Framework			
	a.	The "AID" field value MUST be the AID of OOR Person.	X; requirement in Credential Framework			X; Credential format in vLEI software
	b.	The "LEI" field value MUST be the LEI of Legal Entity Holder.	X; requirement in Credential Framework			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; requirement in Credential Framework			X; Credential format in vLEI software
	d.	The "officialRole" field value MUST be the Official Role specified in the vLEI OOR Credential.	X; requirement in Credential Framework			X; Credential format in vLEI software
10.2 Schema QVI ECR AUTH vLEI Credential	1.	The QVI 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; requirement in Credential Framework			X; Credential format in vLEI software
	2.	The field values in the credential MUST be as follows:	X; requirement in Credential Framework			X; Credential format in vLEI software
	a.	The "AID" field value MUST be the AID of ECR Person.	X; requirement in Credential Framework			X; Credential format in vLEI software
	b.	The "LEI" field value MUST be the LEI of Legal Entity Holder.	X; requirement in Credential Framework			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; requirement in Credential Framework			X; Credential format in vLEI software
	d.	The "engagementContextRole" field value MUST be the Engagement Context Role specified in the vLEI ECR Credential.	X; requirement in Credential Framework			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 QVI ECR AUTH vLEI Credential.	X; requirement in Credential Framework			X; Credential format in vLEI software

verifiable LEI (vLEI) Ecosystem Governance Framework v2.0 Trust Assurance Framework — Document Version 1.4 final — 2024-04-10

Spreadsheet Version Date: 2024-04-10 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; requirement in Credential Framework		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 8.1. Additional schema elements may be added depending on the requirement of a use case.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in vLEI software
	2.	include the Claims marked as Required in section 8.1.			X; assessment and demonstration of Qualified vLEI Issuer compliance	X; Credential format in vLEI software
6.3 Legal Entity Identity Verification	1. Identity Assurance					
	a.	A QVI Authorized Representative (QAR) MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the Credential has been made.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity has 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 Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
6.5 OOR Person Identity Verification						
	6.5.1. 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; requirement in Credential Framework			
	b.	Identity Assurance of a person serving in an Official Organizational Role (OOR Person) MUST be performed prior to authorization of the issuance of an OOR vLEI Credential.	X; requirement in Credential Framework			
	e.	Identity Assurance of an OOR person MUST be performed to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html). Even when IAL2 is used for Identity Assurance, a real-time OOBI session is required (essentially including the IAL3 requirement for a Supervised Remote In-person session).	X; requirement in Credential Framework			
	f.	Upon completion of Identity Assurance, the LAR MUST obtain the consent of the OOR Person for their name and OOR to be published on the on the LEI page of the Legal Entity on gleif.org. This confirmation will be indicated in the QVI QUTH OOR vLEI credential.	X; requirement in Credential Framework			X; Credential format in vLEI software

	g.	The LAR MUST request the OOR Person to generate its AID.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	h.	Then the following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in Credential Framework			
	i.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in Credential Framework			
	i.	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; requirement in Credential Framework			
	ii.	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; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	iii.	The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OOR Person MUST acknowledge that this action has been completed.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	iv.	The LAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	v.	When the response to the Challenge Message has been received by the LAR, the LAR MUST verify the OOR Person's signature.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	j.	The LAR MUST issue a Legal Entity OOR AUTH vLEI Credential to the QVI as required in the Legal Entity QVI AUTH vLEI Credential Framework.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	k.	jThe LAR MUST follow the usage rules below for specifying OOR long names in Legal Entity OOR AUTH vLEI Credentials.	X; requirement in Credential Framework			
	i.	The OOR long name MUST be specified in the Legal Entity OOR AUTH vLEI Credential.	X; requirement in Credential Framework			
	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; requirement in Credential Framework			
	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; requirement in Credential Framework			
	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; requirement in Credential Framework			
	l.	The QVI OOR AUTH vLEI Credential MUST be signed by a threshold satisfying number of LARs using the Legal Entity vLEI Credential.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with 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; requirement in Credential Framework			
	i.	A QAR MUST perform Identity Verification of the Legal Entity as specified in section 6.3 above.	X; requirement in Credential Framework		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 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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iii.	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., such as Board minutes or resolutions, statutes or articles, which would validate the name and the role of the OOR Person.	X; requirement in Credential Framework		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, such as Board minutes or resolutions, statutes or articles, which would validate the name and the role of the OOR Person.	X; requirement in Credential Framework		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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b. Identity Authentication by a QAR					
	i.	A QAR and the OOR Person MUST establish a real-time OOBI session in which the QAR and the OOR Person are present. An example is a continuous web meeting attended by all parties on both audio and video.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	ii.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iii.	A QAR MUST perform manual verification of the OOR Person's legal identity for which the LAR, or third-party service provider, already has performed Identity Assurance. An example: the OOR Person visually presents one or more legal identity credentials verified during Identity Assurance to the QAR.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iv.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	c.	The following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software

	iii.	The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OOR Person MUST acknowledge that this action has been completed.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	iv.	The QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	v.	When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the OOR Person's signature.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	6.5.2 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; requirement in Credential Framework			
	b.	While maintaining the same real-time OOBI session with the QAR during which the Legal Entity vLEI Credential was issued, the OOR Person MUST generate its AID. The OOR Person already has been identity assured in its role as a LAR.	X; requirement in Credential Framework			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; requirement in Credential Framework			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; requirement in Credential Framework			
	1.	The OOR long name MUST be specified in the Legal Entity OOR AUTH vLEI Credential.	X; requirement in Credential Framework			
	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; requirement in Credential Framework			
	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; requirement in Credential Framework			
	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; requirement in Credential Framework			
	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; requirement in Credential Framework			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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	

	iii.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b. Identity Verification by a QAR					
	i.	If the issuance of the OOR vLEI Credential will proceed, a QAR and the OOR Person MUST establish a real-time OOBI session in which the QAR and the OOR Person are present. An example is a continuous web meeting attended by all parties on both audio and video.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	ii.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in Credential Framework			
	iii.	A QAR MUST perform manual verification that the OOR Person is the sole authorized signer who previously generated the AID and, as LAR, issued the Legal Entity OOR AUTH vLEI Credential to the QVI.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	iv.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	c.	The following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	iii.	The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OOR Person MUST acknowledge that this action has been completed.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	iv.	The QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	v.	When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the OOR Person's signature.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
6.6 Issuance	1.	The Legal Entity and OOR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before OOR vLEI Credential issuance can begin.	X; requirement in Credential Framework		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 Official Organizational Role Codes and Reference Data included in OOR vLEI Credentials.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	a.	The QAR MUST confirm that the LAR followed the usage rules specified in section 6.5.1.j. or 6.5.2.c. for including the OOR long name in the Legal Entity OOR AUTH vLEI Credential.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	If the OOR long name specified in the OOR vLEI Credential does not match the OOR long name in the Legal Entity OOR AUTH vLEI Credential, then the QAR MUST not issue the OOR vLEI Credential.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	Usage rules for QARs for abbreviations of OOR roles	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	If an OOR abbreviation exists for an OOR role:	X; requirement in Credential Framework		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; requirement in Credential Framework		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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	c.	Usage rule for QARs for OOR codes	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	i.	If an OOR Role is part of the ISO 5009 Official Organization Role lists, then the OOR code assigned for this OOR role MUST be included in the OOR vLEI credential. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	d.	Usage rule for QARs for the Latin Transliteration of OOR long names	X; requirement in Credential Framework		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; requirement in Credential Framework		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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	4.	A QAR MUST call the vLEI Reporting API with each issuance event of OOR vLEI Credentials.	X; requirement in Credential Framework		X; assessment and demonstration of GLEIF and Qualified vLEI Issuer compliance	
	5.	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; requirement in Credential Framework		X; assessment and demonstration of GLEIF compliance	
6.7 Revocation	1.	To revoke an OOR vLEI Credential:				
	a.	The Legal Entity MUST notify the QVI to revoke an OOR vLEI Credential.	X; requirement in Credential Framework		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; requirement in Credential Framework			X; covered as part of the Credential revocation process with vLEI software
	c.	The QAR then MUST revoke the OOR vLEI Credential.	X; requirement in Credential Framework		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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	2.	A QAR MUST call the OOR Reporting API with each revocation event of Legal Entity Official Organizational Role vLEI Credentials.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	3.	If the QVI has been terminated:				
	a.	At the end of the Grace Period for the Qualified vLEI Issuer vLEI Credential that has been revoked by GLEIF, the QVI MUST revoke all of the OOR vLEI Credentials that the QVI has issued.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with vLEI software
	b.	Then, the terminated QVI MUST transfer a copy of its revocation log to GLEIF.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	4.	GLEIF MUST update the list of OOR vLEI Credentials on the LEI page of the Legal Entity to reflect vLEI credential revocations that have been reported by QVIs.	X; requirement in Credential Framework		X; assessment and demonstration of GLEIF compliance	
6.9 Monitoring	1.	GLEIF MUST monitor the QVI Transaction Event Logs (TELs) to detect the issuance of OOR vLEI Credentials which were not reported using the vLEI Reporting API.	X; requirement in Credential Framework		X; assessment and demonstration of GLEIF compliance	
9 Credential Definition						
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; requirement in Credential Framework			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; requirement in Credential Framework			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; requirement in Credential Framework			X; Credential format in vLEI software
	c.	The "officialRole" field value MUST be the Official Organizational Role itself.	X; requirement in Credential Framework			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; requirement in Credential Framework			X; Credential format in vLEI Software

Spreadsheet Version Date: 2024-04-10 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; requirement in Credential Framework		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; requirement in Credential Framework			
		The Issuer MUST:				
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; requirement in Credential Framework			X; Credential format in vLEI software
	2.	include the Claims marked as Required in section 9.1.	X; requirement in Credential Framework			X; Credential format in vLEI software
6.3 Legal Entity Identity Verification						
	6.3.1. For issuance by a QVI:					
	1. Identity Assurance					
	a.	A QVI Authorized Representative (QAR) MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the Credential has been made.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity has 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 Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
6.4. Legal Entity Authorized Representative (LAR) Identity Verification						
	6.4.2. For issuance by a Legal Entity:					
	1.	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; requirement in Credential Framework			

6.5 ECR Person Identity Verification						
	6.5.1. 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					
	a.	A credential wallet MUST be set up for the ECR Person.	X; requirement in Credential Framework			
	b.	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.	X; requirement in Credential Framework			
	e.	Identity Assurance of an ECR person MUST be performed to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html). Even when IAL2 is used for Identity Assurance, a real-time OOBI session is required (essentially including the IAL3 requirement for a Supervised Remote In-person session).	X; requirement in Credential Framework			
	f.	Upon completion of Identity Assurance, the LAR MUST request the ECR Person to generate its AID.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	g.	Then the following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in Credential Framework			
	h.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in Credential Framework			
	i.	The LAR MUST use an OOBI protocol (such as a QR code or live chat) to share the Legal Entity AID with the ECR Person.	X; requirement in Credential Framework			
	ii.	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 OOBI session.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	iii.	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; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	iv.	The LAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software

	v.	When the response to the Challenge Message has been received by the LAR, the LAR MUST verify the ECR Person's signature.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	i.	The LAR MUST issue a Legal Entity ECR AUTH vLEI Credential to the QVI as required in the Legal Entity QVI AUTH vLEI Credential Framework.	X; requirement in Credential Framework			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 Authentication by a QAR				
	i.	A QAR and the ECR Person MUST establish a real-time OOBI session in which the QAR and the ECR Person are present. An example is a continuous web meeting attended by all parties on both audio and video.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iii.	A QAR MUST perform manual verification of the ECR Person's legal identity for which the LAR, or third-party service provider, already has performed Identity Assurance. An example: the ECR Person visually presents one or more legal identity credentials verified during Identity Assurance to the QAR.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iv.	A QAR MUST ask the ECR Person verbally to confirm the AID that was sent in the Legal Entity ECR AUTH vLEI Credential. If the AID provided by the ECR Person does not match the AID sent in the Legal Entity ECR AUTH vLEI Credential, the OOBI session ends.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	b.	The following steps MUST be performed in this order and completed during this OOBI session.				
	i.	The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the ECR Person.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	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 OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	iii.	The ECR Person MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the ECR Person MUST acknowledge that this action has been completed.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	iv.	The QAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	v.	When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the ECR Person's signature.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	6.5.2 For issuance by a QVI for a Legal Entity with a sole 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; requirement in Credential Framework			
	b.	Since the ECR Person also is the only LAR, the single employee as the LAR MUST issue a Legal Entity ECR AUTH vLEI Credential to the QVI.	X; requirement in Credential Framework			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.	QAR and the ECR Person MUST establish a real-time OOBI session in which the QAR and the ECR Person are present. An example is a continuous web meeting attended by all parties on both audio and video.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	b.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	c.	A QAR MUST ask the ECR Person verbally to confirm the AID that was sent in the Legal Entity ECR AUTH vLEI Credential. If the AID provided by the ECR Person does not match the AID sent in the Legal Entity ECR AUTH vLEI Credential, the OOBI session ends.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	e.	Identity Assurance				
	i.	Identity Assurance of the ECR Person who is the sole employee MUST be performed prior to the issuance of an ECR vLEI Credential.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	ii.	Identity Assurance of an ECR Person that is a sole employee MUST be performed either by a QAR or through the use of Third-Party Services by the QVI since an ECR Person that is a sole employee is unable to identity assurance itself.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iv.	Identity Assurance of an ECR person MUST be performed to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html). Even when IAL2 is used for Identity Assurance, a real-time OOBI session is required (essentially including the IAL3 requirement for a Supervised Remote In-person session).	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	f.	Identity Authentication				
	i.	The following steps MUST be performed in this order and completed during this OOBI session.				
	ii.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iii.	The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the ECR Person.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	iv.	The QAR MUST send a Challenge Message to the ECR Person's AID as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of the ECR Person's AID. The Challenge Message MUST be unique to the OOBI session.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	v.	The OOR 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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	vi.	The QAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	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 QAR, the QAR MUST verify the ECR Person's signature.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential issuance process with vLEI software
	6.5.3 For issuance by a Legal Entity with more than one authorized signer or employee					

	1. Identity Assurance					
	a.	A LAR, or a Third-Party Services engaged by the Legal Entity, MUST perform Identity Assurance of a person serving in an Engagement Context Role (ECR Person) to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html). Even when IAL2 is used for Identity Assurance, a real-time OOBI session is required as specified 2.b below (essentially including the IAL3 requirement for a Supervised Remote In-person session).	X; requirement in Credential Framework			
	2. Identity Authentication					
	a.	A credential wallet MUST be set up for the ECR Person.	X; requirement in Credential Framework			
	b.	A LAR and the ECR Person MUST meet in person or establish a real-time OOBI session in which the LAR and the ECR Person are present. An example is a continuous web meeting attended by all parties on both audio and video.	X; requirement in Credential Framework			
	c.	Video filters and avatars MUST not be used during the OOBI session.	X; requirement in Credential Framework			
	d.	The following steps MUST be performed in this order and completed during this OOBI session.	X; requirement in Credential Framework			
	i.	The LAR MUST perform manual verification of the ECR Person's legal identity for which the LAR has already performed Identity Assurance. An example: the ECR Person visually presents one or more legal identity credentials and the LAR compares to the credentials verified during Identity Assurance.	X; requirement in Credential Framework			
	ii.	The LAR MUST use an OOBI protocol (such as a QR code or live chat) to share the Legal Entity AID with the ECR Person.	X; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
	iii.	The ECR Person MUST use an OOBI protocol (such as a QR code or live chat) to share its AID with the LAR.	X; requirement in Credential Framework			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 OOBI session.	X; requirement in Credential Framework			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; requirement in Credential Framework			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; requirement in Credential Framework			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; requirement in Credential Framework			X; covered as part of the Credential issuance process with vLEI software
6.6 Issuance						
	6.6.1 For issuance by a QVI:					
	1.	The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before ECR vLEI Credential issuance can begin.	X; requirement in Credential Framework		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, prior to issuing and signing an ECR vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR. Another QAR then approves the issuance and signs the ECR vLEI Credential.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	6.6.2 For issuance by a Legal Entity:					
	1.	The ECR Person Identity Verification process outlined in section 6.5 MUST be completed before ECR vLEI Credential issuance can begin .	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	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.	X; requirement in Credential Framework			
6.7 Revocation						
	6.7.1. For revocation by a QVI:					

	1.	The Legal Entity MUST notify the QVI to revoke an ECR vLEI Credential.	X; requirement in Credential Framework			
	2.	To revoke a previously issued ECR vLEI Credential, the LAR(s) MUST revoke the QVI AUTH ECR vLEI Credential related to a specific issuance of an ECR vLEI Credential.	X; requirement in Credential Framework		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; requirement in Credential Framework		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; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	X; covered as part of the Credential revocation process with vLEI software
	5.	At the end of the Grace Period for the Qualified vLEI Issuer vLEI Credential that has been revoked by GLEIF, the QVI MUST revoke all of the ECR vLEI Credentials that the QVI has issued.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
	6.	Then the terminated QVI MUST transfer a copy of its revocation log to GLEIF.	X; requirement in Credential Framework		X; assessment and demonstration of Qualified vLEI Issuer compliance	
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; requirement in Credential Framework			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; requirement in Credential Framework			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; requirement in Credential Framework			X; Credential format in vLEI software
	c.	The "engagementContextRole" field value MUST be the Engagement Context Role.	X; requirement in Credential Framework			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 QVI AUTH vLEI Credential (via SAID) that the issuing QVI received authorizing the issuance of this ECR 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; requirement in Credential Framework			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; requirement in Credential Framework			X; Credential format in vLEI software