Enabling global identity
Protecting digital trust

verifiable LEI (vLEI)
Ecosystem Governance Framework v1.0

Glossary

Public
Document Version 1.0
2022-12-16

Version	1.0
Date of version	2022-12-16
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework Glossary
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2022-12-16_verifiable-LEI-(vLEI)-Ecosystem-Governance-Framework-Glossary_v1.0_final.docx
Governing Authority	Global Legal Entity Identifier Foundation (GLEIF)
Copyright	The verifiable LEI (vLEI) Ecosystem Governance Framework is published on the GLEIF website. All documents published on the GLEIF website are published under the Creative Commons Attribution license.

1 Introduction

This is a Controlled Document of the verifiable LEI (vLEI) Ecosystem Governance Framework (vLEI Ecosystem Governance Framework). It is the Glossary for the vLEI Ecosystem Governance Framework.

2 Glossary Terms and Definitions

All terms in First Letter Capitals in the (vLEI) Ecosystem Governance Framework Primary Document and Controlled Documents are defined in the vLEI Ecosystem Governance Framework Glossary. Additional terms will continue to be added.

Terms	Definitions
Active Status	A LEI Entity status in the Global LEI System.
Annual vLEI Issuer Qualification	A formal annual evaluation process performed by GLEIF to ensure that the Qualified vLEI Issuer continues to meet the requirements of the vLEI Ecosystem Governance Framework.
Audit Report	An audit report provided to the Qualified vLEI Issuer by its internal or external auditors or comparable function.

Candidate vLEI Issuer	An organization that has applied to become a Qualified vLEI Issuer.
Continuity Policy	A policy that GLEIF must have for the survival of control authority of all controllers for the GLEIF Root AID and its Delegated AIDs, including Escrow Controllers and that QVIs and Legal Entities should have for survival of control authority of their Controllers.
Day	A business day, provided that a given day only counts as such if it is a business day both at GLEIF's legal domicile in the operating office in Frankfurt/Germany, and at the Qualified vLEI Issuer's domicile. Defined term in the vLEI Issuer Qualification Agreement.
Designated Authorized Representatives (DARs)	A representative of a Qualified vLEI Issuer or a Legal Entity that are authorized by the QVI or the Legal Entity to act officially on behalf of the QVI or the Legal Entity. DARs of QVIs can authorize vLEI Issuer Qualification Program Checklists, execute the vLEI Issuer Qualification Agreement and provide designate/replace Qualified vLEI Issuer Authorized Representatives (QARs). DARs of Legal Entities can execute the contract between a Qualified vLEI Issuer and the Legal Entity and provide designate/replace Legal Entity Authorized Representatives (LARs).
Effective Date	The later of the dates of signing shown on the first page of the vLEI Issuer Qualification Agreement.
Engagement Context Role Person (ECR Person)	A person that represents the Legal Entity in a functional or in another context role and is issued an ECR vLEI Credential.
Extraordinary vLEI Issuer Qualification	Qualification conducted under exceptional circumstances which give GLEIF reason to believe that the Qualification Documentation is no longer current or being adhered to
GLEIF	Global Legal Entity Identifier Foundation
GLEIF Authorized Representative (GAR)	A representative of GLEIF authorized to perform the identity verification requirements needed to issue the QVI vLEI Credential. GLEIF has authorized specific GARs, Internal and External GARs, for the GIDA and GEDA (see definition of Delegated AIDs).

GLEIF Business Day	Business Day in Frankfurt am Main, Germany (Monday – Friday).
GLEIF Identifier Governance Framework, v1.0	A document that details the purpose, principles, policies, and specifications that apply to the use of the GLEIF Root Autonomic Identifier (AID) and its GLEIF Delegated AIDs in the vLEI Ecosystem.
GLEIF Website	http://www.gleif.org
GLEIS	Global Legal Entity Identifier System
Global LEI Repository	A database managed by GLEIF containing all current and historical LEIs and LEI reference data.
Identity Assurance	A process that is part of Identity Verification, the steps of which are defined in each of the vLEI Credential Frameworks of the vLEI Ecosystem Governance Framework, which must be conducted before the issuance of vLEI Credentials.
Identity Authentication	A process that is part of Identity Verification, the steps of which are defined in each of the vLEI Credential Frameworks of the vLEI Ecosystem Governance Framework, which must be conducted before the issuance of vLEI Credentials.
Legal Entity	As defined in ISO 17442:2020, a legal person or structure that is organized under the laws of any jurisdiction; includes, but is not limited to, unique parties that are legally or financially responsible for the performance of financial transactions or have the legal right in their jurisdiction to enter independently into legal contracts, regardless of whether they are incorporated or constituted in some other way (e.g., trust, partnership, contractual). It includes governmental organizations and supranationals and individuals when acting in a business capacity but excludes natural persons. It also includes international branches.
Legal Entity Authorized Representative (LAR)	A representative of a Legal Entity that are authorized by a DAR of a Legal Entity to request issuance and revocation of vLEI Legal Entity Credentials, Legal Entity Official Organizational Role vLEI Credentials (OOR vLEI Credentials), and Legal Entity Engagement Context Role vLEI Credentials (ECR vLEI Credentials).

Legal Entity Engagement Context Role vLEI Credential Governance Framework	A document that details the requirements for vLEI Role Credentials issued to representatives of a Legal Entity in other than official roles but in functional or other context of engagement.
Legal Entity Official Organizational Role vLEI Credential Governance Framework	A document that details the requirements for vLEI Role Credentials issued to official representatives of a Legal Entity.
Legal Entity vLEI Credential Governance Framework	A document that details the requirements for vLEI Credential issued by a Qualified vLEI Issuer to a Legal Entity.
LEI Issuer	An organization accredited by GLEIF to validate legal entity information and register new LEIs and reference data which are sent to GLEIF for inclusion in the GLEIS.
LEI, LEIs	Legal Entity Identifier(s)
Non-Disclosure Agreement (NDA)	An agreement that outlines requirements for handling confidential information (Appendix 1 to the vLEI Issuer Qualification Agreement)
Official Organizational Role Person (OOR Person)	A person that represents the Legal Entity in an official organizational role and is issued an OOR vLEI Credential.
Out-of-band Interaction (OOBI)	A session, an example is a continuous web meeting attended by all parties on both audio and video.
pdf, pdf-document	A document in the standard portable document format "pdf"-format
Qualification	The formal evaluation process performed by GLEIF to ensure that an organization which has applied for Qualification (a Candidate vLEI Issuer) meets the requirements of the vLEI Ecosystem Governance Framework.
Qualification Documentation	The documentation to be provided by the Candidate or Qualified vLEI Issuer to GLEIF for evaluation for Qualification.
Qualified vLEI Issuer – Legal Entity Required Contract Terms	A document that specifies the contract terms that must be included in the agreement between a Qualified vLEI Issuer and a Legal Entity that has

	requested a Legal Entity vLEI. (Appendix 7 to the vLEI Issuer Qualification Agreement)
Qualified vLEI Issuer (QVI)	The contracting party to the vLEI Issuer Qualification Agreement that has been qualified by GLEIF as a Qualified vLEI Issuer.
Qualified vLEI Issuer Authorization vLEI Credential	A vLEI credential that enables simple, safe, secure instruction and authorization by a Legal Entity Authorized Representative (LAR) sent to a QVI for the issuance and revocation of vLEI Role Credentials.
Qualified vLEI Issuer Authorized Representative (QAR)	A designated representative of a QVI authorized to conduct QVI operations with GLEIF and Legal Entities. QARs perform the Identity Verification requirements needed to issue vLEI Legal Entity Credentials, Legal Entity Official Organizational Role vLEI Credentials (OOR vLEI Credentials), and Legal Entity Engagement Context Role vLEI Credentials (ECR vLEI Credentials) as well as the issuance and revocation these Credentials.
Qualified vLEI Issuer Business Day	Business Day according to local Qualified vLEI Issuer business calendar.
Qualified vLEI Issuer Identifier and vLEI Credential Governance Framework	A document that details the requirements to create and delegate AIDs for the QVI and to enable the vLEI Credential to be issued by GLEIF to Qualified vLEI Issuers which allows the Qualified vLEI Issuers to issue, verify and revoke Legal Entity vLEI Credentials, Legal Entity Official Organizational Role vLEI Credentials, and Legal Entity Engagement Context Role vLEI Credentials.
Qualified vLEI Issuer TrustMark Terms of Use	A document that details the terms of use of the TrustMark by the Qualified vLEI Issuer. (Appendix 6 to the vLEI Issuer Qualification Agreement)
QVI Authorized Representative (QAR)	A designated representative of a QVI authorized to conduct QVI operations with GLEIF and Legal Entities.
QVI Authorized Representative (QAR) Person	A person in the role of a QAR.
Root of Trust	Strong governance which begins with the issuance and maintenance of the LEI itself, GLEIF will be the anchor of the vLEI ecosystem, at the root of the governance that will position the LEI as a key component in building a trust layer for identification and verification of legal entities as the LEI allows authentication that the legal entity is indeed who it claims to be and that those who act on its behalf, can.

Service Level Agreement (SLA)	A document that contains detailed descriptions of the services to be provided by GLEIF and Qualified vLEI Issuers and the service level requirements expected for these services. (Appendix 5 to the vLEI Issuer Qualification Agreement)
Solicited Issuance	The issuance of a Legal Entity vLEI Credentials, OOR vLEI Credentials and ECR vLEI Credentials upon receipt by the QAR of a Fully Signed issuance request from the LARs.
Swiss Law	A set of rules, orders, regulation and court decisions which constitutes the law in Switzerland. The source of Swiss law can be federal or cantonal. GLEIF will host a list of links where Swiss law can be found.
Third Party Services	IT or operational infrastructure services outsourced by Qualified vLEI Issuers.
TrustMark	A TrustMark for a Qualified vLEI Issuer provided GLEIF by to the Qualified vLEI Issuer (refer to Appendix 6 to the vLEI Issuer Qualification Agreement)
Unsolicited Issuance	Issuance of a Legal Entity vLEI Credential upon notice by a QAR to the LARs that a Legal Entity vLEI Credential has been solicited on the Legal Entity's behalf.
verifiable LEI (vLEI)	An Authentic Chained Data Container credential which contains an LEI issued in accordance with the vLEI Ecosystem Governance Framework requirements.
verifiable LEI (vLEI) Ecosystem Governance Framework Information Trust Policies	A document that defines the information security, privacy, availability, confidentiality and processing integrity policies that apply to all vLEI Ecosystem Members.
vLEI Chain of Trust	The cryptographic chain of trust for organizational identity established for the vLEI which connects the following entities: GLEIF>Qualified vLEI Issuers>Legal Entities>Persons Representing Legal Entities.
vLEI Ecosystem Stakeholder	A stakeholder in the vLEI Ecosystem following the requirements outlined in the vLEI Ecosystem Governance Framework.
vLEI Issuance	The process of issuing a vLEI Credential.

vLEI Issuer Contact Details	A list of contact details of GLEIF and the Candidate vLEI Issuer during Qualification and of GLEIF and the Qualified vLEI Issuer during ongoing operations. Also, will include the names and email addresses of Designated Authorized Representatives (DARs) of the Legal Entity (Appendix 4 to the vLEI Issuer Qualification Agreement).
vLEI Issuer Qualification Agreement	An agreement between GLEIF and an organization that has been qualified by GLEIF to operate as a Qualified vLEI Issuer.
vLEI Issuer Qualification Program Checklist	The document that details the control and process requirements for Qualification (Appendix 3 to the vLEI Issuer Qualification Agreement).
vLEI Issuer Qualification Program Manual	The document that describes the Qualification program (Appendix 2 to the vLEI Issuer Qualification Agreement).
vLEI Maintenance	All steps taken to ensure that the vLEI continues to be based on the existence of a LEI that maintains the required entity and registration statuses in the GLEIS as well as keeping credential wallets and private keys secure.
vLEI Revocation	The process of revoking a vLEI Credential.
vLEI User	Any user of vLEI credentials in any applicable use case.

Technical Terms	Technical Definitions
Autonomic Identifiers (AIDs)	AIDs are self-certifying identifiers that are imbued with self-management capabilities via the KERI protocol. There are two main classes of AIDs in KERI: 1) transferable AIDS, and 2) non-transferable AIDS. Key management policies are different for the two classes of AIDs.
Challenge Message	A message sent and responded to during the Identity Authorization session.
Controller	A controlling entity of an identifier. See the examples Root AID GLEIF Authorized Representative, the Internal Delegated AID GLEIF Authorized Representative and the External Delegated AID GLEIF Authorized Representative in the GLEIF Identifier Governance Framework.
Delegated AIDs	Autonomic Identifiers (AIDs) which have associated Decentralized Identifier (DIDs). These are primary identifiers. Unless otherwise indicated, whenever the term identifier is used with reference to KERI, the references are to primary identifiers. Examples are: GLEIF Internal Delegated AID (GIDA) and GLEIF External Delegated AID (GEDA).
Distributed Hash Table (DHT)	In computing, a data structure that implements an associative array abstract data type, a structure that can map keys to values (Wikipedia). Within the vLEI Ecosystem, these tables are used for the discovery of AIDs.
Escrow Agent	Specific organizations appointed by GLEIF as secondary signers to the GLEIF Root AID, to be able to act if the required weighted multi-sig threshold of GLEIF primary signers is not available for key rotation or recovery.
Fully Signed	Meets the threshold of the signed keys
GLEIF API	API to directly access the complete LEI data pool in real time with rich query capabilities. QVIs must use the GLEIF API to look up the Registration Status of LEIs, to ensure that vLEI credentials are only issued to organizations who have an LEI in good standing and to identify, if vLEI credentials have to be revoked because the LEI has LAPSED or is otherwise not in good standing anymore.

GLEIF Root of Trust AID	The GLEIF Root Aid provides the Root of Trust for the ecosystem tree of trust. Each branch in that tree is a Chain of Trust. The Delegated Aid Chain of Trust branch provides trust for delegated GLEIF AIDS and Qualified vLEI Issuer Delegated AIDs. The vLEI Chain of Trust branch, that attaches to the Delegated AID Chain of Trust branch, provides trust for all vLEIs within the vLEI ecosystem.
Inception Event	Initial event used during the creation of an AID.
Interaction Event	Non-establishment Event that anchors external data to the key-state as established by the most recent prior establishment event.
IT	Information Technology, encompassing application software, computer and network systems and suitable equipment for the implementation and support of such systems.
Judge	an entity or component that examines the entries of the one or more Key Event Receipt Logs (KERLs) and Duplicitous Event Logs (DELs) of given identifier to validate that the vent history is from a non-duplicitous Controller and has been witnessed by a sufficient number of non-duplicitous Witnesses such that it may be trusted or conversely not-trusted by a Validator.
Juror	An entity or component that performs duplicity detection on events and event receipts. A Juror is the Controller of its own self-referential identifier which may or may not be the same as the identifier to which it is a Juror. The Juror may thereby create digital signatures on statements about duplicity it has detected.
Key Event Receipt Infrastructure (KERI)	Provides the identifier and key management architecture for the vLEI Ecosystem Technical Architecture *(Link to KERI white paper: Smith, S. M., "Key Event Receipt Infrastructure (KERI) Design", Revised 2020/09/06, 2019/07/03)*

Key Management	Unless otherwise specified, the term *key-pair* refers to an asymmetric (public, private) key-pair for digital signatures. The private key is used to generate signatures and the public key is used to validate signatures. Ecosystem key management policies are grouped into three sets of policies for protecting three different infrastructures. 1. Key-pair creation and storage infrastructure; 2. Signature creation infrastructure; 3. Signature verification infrastructure.
Key Pre-Rotation for Transferable AIDs	KERI, the authoritative key stage of a transferable AID consists of two sets of key-pairs. The first set is the current set of signing keys and the second set is the pre-committed set of one-time rotation keys that after rotation will become the next or pre-rotated set of signing keys. These two sets provide the basis for KERI's pre-rotation mechanism. the on device storage of public/private key pairs associated with an AID.
Key Store	The on-device storage of public/private key pairs associated with an AID.
Non-Transferable AIDs	Non-transferable AIDs are self-certifying but are not meant for long term persistent use and hence their key-pair(s) are not rotatable. Instead, the identifier is abandoned and replaced with a new identifier with a new set of key-pair(s). These may also be called ephemeral AIDs. Within KERI, the primary use for non-transferable (ephemeral) AIDs are for the Witness identifiers. Because Witnesses are used in a pool, the pool forms a threshold structure which provides protection from the exploit of a minority of the key-pairs of the ephemeral Witness AIDs in the pool. If a given Witness AID has its key(s) compromised, then the Witness AID itself is abandoned and replaced. Thus, the Witness pool management policy protects Witness ephemeral AIDs.
Proof Request	One of the initiating steps in the Issuance and Presentation Exchange Protocol (IPEX). In this step, a Verifier is requesting a credential presentation from a holder of a credential as proof that the holder is in possession of a credential that meets criterial defined in the proof request.
Registrar (Ledger)	In place of a traditional KERI witness pool a blockchain (i.e, Cardano) or other Distributed Ledger Technology (DLT) can be used to store Key Events.

Resolver	An entity or component that provides discovery for identifiers. A Resolver is the Controller of its own self-referential identifier which may not be the same as the identifier to which it is a Resolver.
Rotation Event	An event to rotate AIDs
Seal	A cryptographic commitment in the form of a cryptographic digest or hash tree root (Merkle root) that anchors arbitrary data or a tree of hashes of arbitrary data to a particular event in the key event sequence.
Service Endpoints	Address at where a given identifier can receive KERI messages.
Signature Verification Infrastructure	An attack against signature verification infrastructure typically requires replacing the signature verification code with malicious code that falsely reports signature verification on signed statements. KERI provides a specific protection mechanism for signature verification via a Watcher pool where an event is only accepted as verified if a sufficient majority of the Watchers in a pool agree on the verification status of the signature(s) on that event. This provides a threshold structure where an attacker must compromise the code integrity of a sufficient number of Watchers for successful attack. Because the composition of a Watcher pool does not need to be publicly disclosed, an attacker must also discover that composition to ensure a successful attack.
Sources	The sources or edges section of a vLEI credential cause the vLEI credential to become a fragment of a distributed property graph. The sources chain a vLEI credential to other vLEI credential to which this credential is dependent.
Spot Check	The operation of performing an OOBI exchange and challenge/response exchange over a live session with an unauthenticated contact to ensure the other person in the live session has control of the contact's private keys.
Strength	All key-pairs MUST be generated using a cryptographic algorithm with at least 128 bits of cryptographic strength for the salt or seed used to generate the private key of the key pair.
Validator	An entity or component that determines that a given signed statement associated with an identifier was valid at the time of its issuance.

Verifiable Data Registries (VDRs)	A system mediating the creation and verification of identifiers, keys, and other relevant data (W3C). Within the vLEI Ecosystem, these registries are used for issuance and revocation state of vLEIs.
Verifier	An entity or component that cryptographically verifies the signature(s) on an event message.
vLEI Software	Open-source developed software sponsored by GLEIF with the capabilities for vLEI Credential Issuance, vLEI Credential Presentation, Identifier and Key Management and vLEI Credential Revocation and supporting functions.
Watcher	An entity or component that keeps a copy of a Key Event Receipt Log (KERL) for an identifier but is not designated by the Controller thereof as one of its Witnesses.
Witness	An entity or component designated (trusted) by the Controller of an identifier. The primary role of a Witness is to verify, sign, and keep events associated with an identifier. A Witness is the Controller of its own self-referential identifier which may or may not be the same as the identifier to which it is a Witness. As a special case a Controller may serve as its own Witness. Witness designations are included in key (establishment) events. As a result, the role of a Witness may be verified using the identifier's rotation history. When designated, a Witness becomes part of the supporting infrastructure establishing and maintaining control authority over an identifier. An identifier Witness therefore is part of its trust basis and may be controlled (but not necessarily so) by its Controller.