verifiable LEI (vLEI)Ecosystem Governance Framework Glossary

Document Name:	verifiable LEI (vLEI) Ecosystem Governance Framework Glossary
Document DID:	
Version Number:	V0.6
Version Date:	
Governance Authority:	Global Legal Entity Identifier Foundation (GLEIF)
Governance Authority DID:	
Copyright:	

1 Introduction

This is a Controlled Document of the GLEIF verifiable LEI (vLEI) Ecosystem Governance Framework (vLEI Ecosystem Governance Framework). It is the Glossary for the vLEI Ecosystem Governance Framework. For more information about the vLEI Ecosystem Governance Framework, please see the following section on the GLEIF website at [INSERT URL HERE].

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
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.
Authorized vLEI Representatives (AVRs)	Representatives of a Legal Entity that are authorized by the 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).
Candidate vLEI Issuer	An organization that has applied to become a Qualified vLEI Issuer.
Continuity Policy	Definition to be added
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)	Representatives of a Legal Entity that are authorized by the Legal Entity to act officially on behalf of the Legal Entity. DARs can authorize vLEI Issuer Qualification Program Checklists, execute the vLEI Issuer Qualification Agreement and provide designate/replace Authorized vLEI Representatives (AVRs).
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 an other 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 verifications requirements needed to issue the QVI vLEI Credential.
GLEIF Business Day	Business Day in Frankfurt am Main, Germany (Monday – Friday).
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.
IT	Information Technology, encompassing application software, computer and network systems and suitable equipment for the implementation and support of such systems.
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)*
Legal Entity	As defined in ISO 17442:2020, 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 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, LEIs	Legal Entity Identifier(s)
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.
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 webmeeting attended by all parties on both audio and video.
pdf, pdf-document	A document in the standard portable document format "pdf"-format
Root of Trust	Definition to be added
Service Level Agreement (SLA)	A document that will be developed in preparation for the production launch of the vLEI Ecosystem and Infrastructure and will contain 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)
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 Authorized Representative (QAR)	A representative of the QVI authorized to perform the identity verifications requirements needed to issue the QVI vLEI Credential.
Qualified vLEI Issuer Business Day	Business Day according to local Qualified vLEI Issuer business calendar.
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 vLEI Credential Governance Framework	A document that details the requirements to enable this 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)
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.
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.
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 AVR(s) of the Legal Entity.
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 AVR(s) of the Legal Entity that a Legal Entity vLEI Credential has been solicited on the Legal Entity's behalf.
verifiable LEI (vLEI)	A Verifiable 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 integreity policies that apply to all vLEI Ecosystem Members.
vLEI Chain of Trust	Definition to be added
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 Qualfication Agreement).
vLEI Issuer Qualification Program Manual	The document that describes the Qualification program (Appendix 2 to the vLEI Issuer Qualfication Agreement).
vLEI Ecosystem Member	A stakeholder in the vLEI Ecosystem following the requirments outlined in the vLEI Ecosystem Governance Framework
vLEI Issuance	The process of issuing a vLEI Credential.
vLEI Maintenance	All steps taken to ensure that the vLEI continues to be based on the existence of a LEI with Issued and Active status 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

12
13

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 fro the two classes of AIDs.
Challenge Message	A message sent and responded to during the Identity Authorization session.
Controllers	Definition to be added

Delegated AID Chain of Trust	Definition to be added
Endorser (Backer) Management	An Endorser provides a secondary root-of-trust for KEL (Key Event Log). Two types of Endorsers will be supported initially: Witnesses and Registrars.
Fully Signed	Meets the threshold of the signed keys
GLEIF External Delegated AID	These policies are used by GLEIF to issue the Qualified vLEI Issuer vLEI Credentials and Qualified vLEI Issuer Delegated AIDs. They are the same as GLEIF Internal Delegated AID policies except: 1. GLEIF MUST set the Do Not Delegate configuration property on Delegated vLEI Issuer AIDs.
GLEIF Internal Delegated AIDs	These policies are used by GLEIF to issue internal vLEIs. They are identitcal to the policies for the GLEIF Root AID except: 1. Key Pair Creation and Storage Infrastruture **SHOULD** be within a TEE. 2. Each key-pair in a threshold multi-sig **SHOULD** use a non-co-located TEE.
GLEIF KERI Distributed Hash Table (DHT)	These policies are for discovery of AIDs within the GLEIF vLEI Ecosystem.
GLEIF Verifiable Data Registries (VDRs)	These policies are for issuance and revocation state of vLEIs and other VCs.
GLEIF Root of Trust AID	Definition to be added
Hybrid (Witness Pool and Ledger Registrar)	MUST use only one type for any KEL; MAY use different types for each Delegated KEL at any level of a delegation hierarchy.
Inception Event	Definition to be added
Interaction Event	See Out-of-band Interaction (OOBI)
Key Event Receipt Infrastructure (KERI)	The protocol that GLEIF and Qualified vLEI Issuers will use for the vLEI Ecosystem.
Key Management	Unless otherwise specified, the term *key-pair* referes 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 a nd storage infrastructure; 2. Signature creation infrastructure; 3. Signature verification infrastructure.
Key Pre-Rotation for Transferable AIDs	In Keri, the authoritative key stae 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-commited 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.
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.
Private Key Store	Definition to be added
Qualified vLEI Issuer Distribution	GLEIF Should encourage and promote a diverse distribution of Qualified vLEI Issuers across political jurisdictions and geographies.
Registrar (Ledger)	SHOULD use only one Registrar at a time for a givel KEL; MUST use a GLEIF Approved DID Method (one for each authorized ledger)
Rotation Event	An event to rotate AIDs
Service Endpoints	Definition to be added
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.
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.
Watcher Management	Validators need to be protected by their Watcher network.
Witness Pool	A Witness is 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.

14
15