GLEIF vLEI Architecture

Samuel M. Smith Ph.D.
version 1.1
sam@prosapien.com
2021-01-04

vLEI = *verifiable* Legal Entity Identifier

A vLEI is a digitally signed digital document that makes assertions about a Legal Entity.
These assertions include the LEI code, official name, and registered address.

Two senses of *verifiable* in vLEI.

- *verifiable veracity* of the assertion in the vLEI
- *verifiable authenticity* of the assertions in the vLEI

GLEIF and its issuing organizations verify the *veracity* (accuracy, validity, quality), of the assertions in vLEIs they issue. Their credibility, operational integrity, process, policy, and procedures provide assurance of veracity.

The digital document format for the vLEI is based on the W3C Verifiable Credential (VC) and Decentralized Identifier (DID) standards. These standards provides interoperable mechanisms for verifying the *authenticity* of the vLEI.
The *verifiable* in VC refers only to the *verifiable authenticity* of the document via the attached digital signatures.
Think of a VC as an authenticatible data container for assertions.
The cryptographic security of the identity systems used to issue the associated DIDs provide assurance of authenticity.

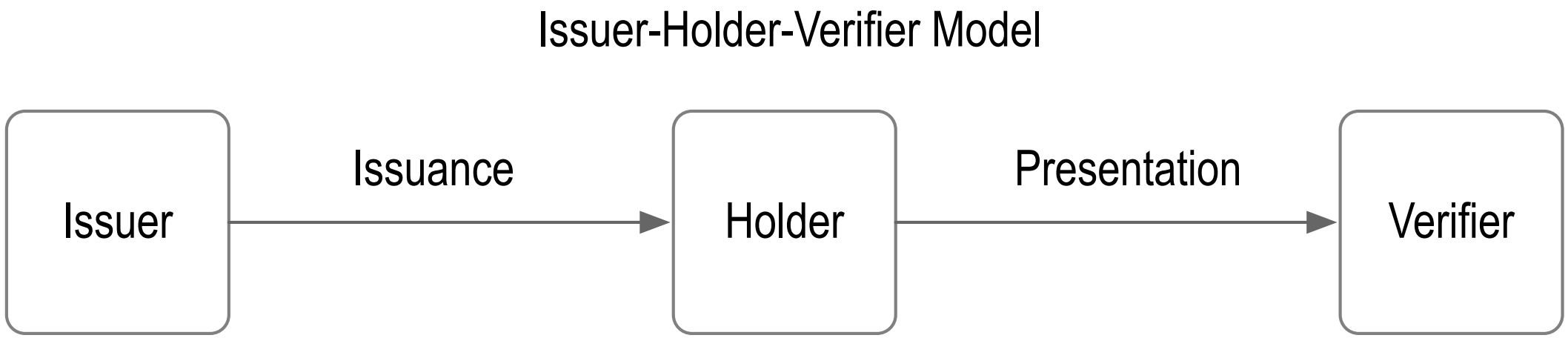
A vLEI issued by a GLEIF authorized issuing organization contains assertions of high data quality about the targeted legal entity.
A vLEI expressed as a VC provides those assertions in a way that is securely authenticatible to the identified issuing organization.

The remainder of these slides provide a brief overview of the cryptographic infrastructure used to provide secure authenticity.

Tripartite Authentic Data (VC) Model

Issuer: Source of the VC. Creates (issues) and signs VC
Holder: Usually the target of the VC. The holder is the "*issuee*" that receives the VC and holds it for its own use.
Verifier: Verifies the signatures on the VC and authenticates the holder at the time of presentation

The issuer and target each have a DID (decentralized identifier).
The DIDs are used to look-up the public key(s) needed to verify signatures.

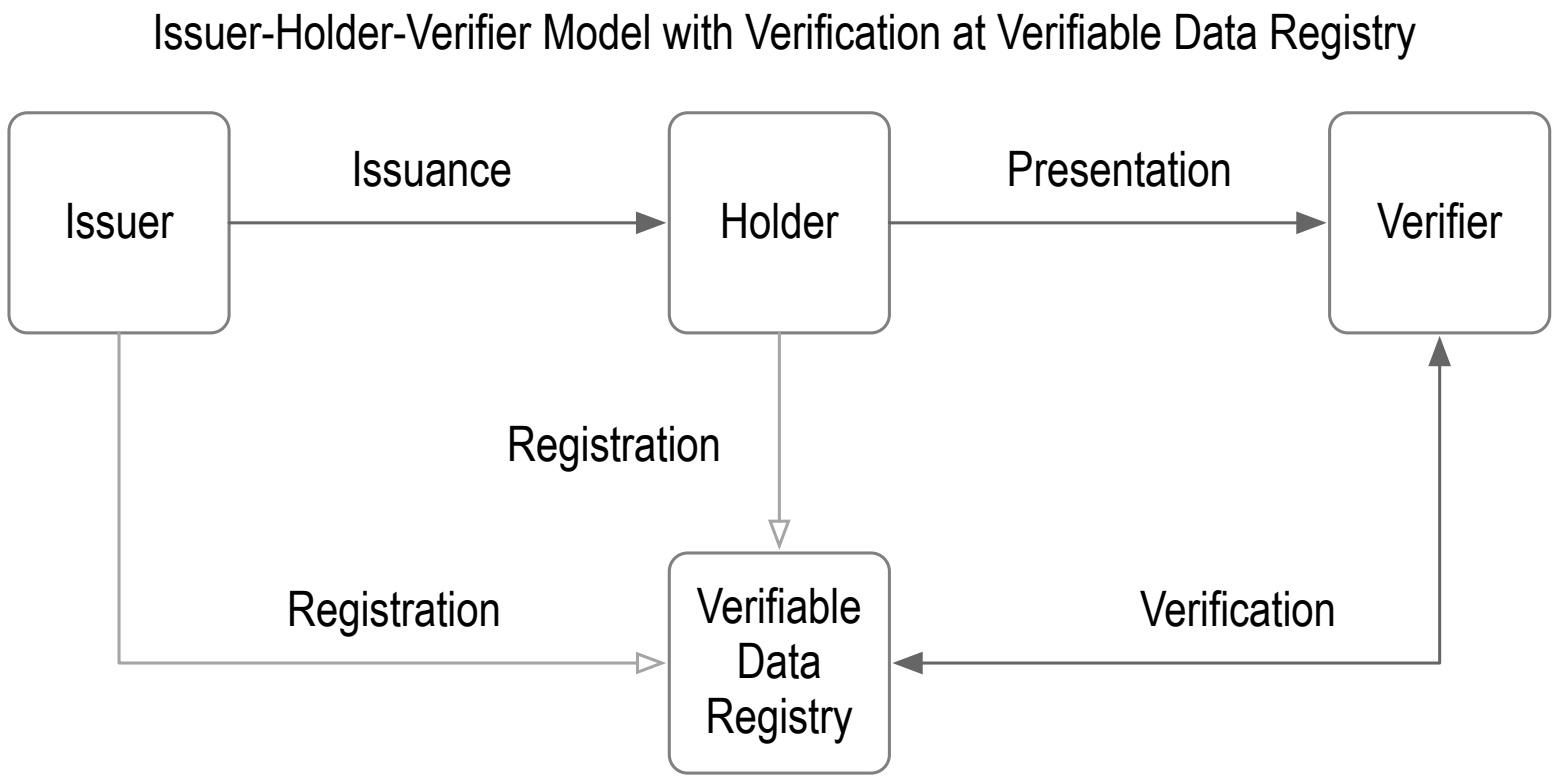


Tripartite Authentic Data (VC) Model with VDR

Verifiable Data Registry (VDR) enables decentralized but interoperable discovery and verification of authoritative key pairs for DIDs in order to verify the signatures on VCs. A VDR may also provide other information such as data schema or revocation state of a VC.

Each controller of a DID registers that DID on a VDR so that a verifier can determine the authoritative key pairs for any signatures.

We call this determination, *establishment of control authority* over a DID.

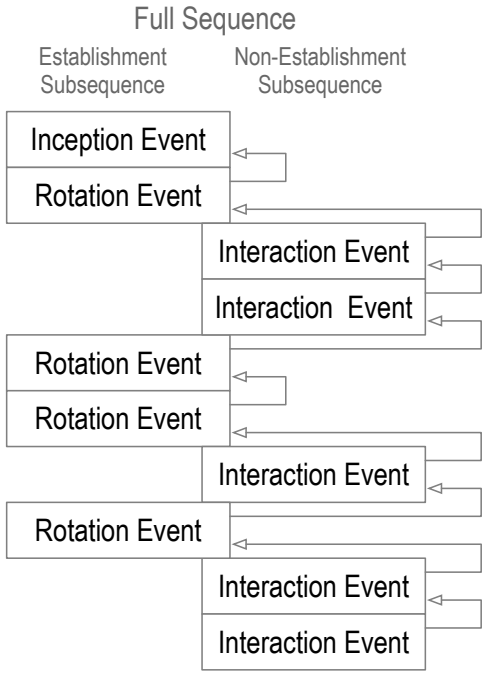


KERI VDRs vs. Shared Ledger VDRs

Most DID methods use a shared ledger (commonly referred to as a *blockchain*) for their VDR. Typically, in order to interoperate all participants must use the same shared ledger or support multiple different DID methods. There are currently over 70 DID methods. Instead GLEIF has chosen to use KERI based DID methods. KERI stands for Key Event Receipt Infrastructure. KERI based VDRs are ledger independent, i.e. not locked to a given ledger. This provides a path for greater interoperability without forcing participants in the vLEI ecosystem to use the same shared ledger.

A KERI VDR is called a key event log (KEL). It is a cryptographically verifiable hash chained data structure. Each KERI based identifier has its own dedicated KEL. The purpose of the KEL is to provide proof of the establishment of control authority over an identifier. This provides cryptographically verifiable proof of the current set of authoritative keys for the identifier. KERI identifiers are long cryptographic pseudo random strings of characters. They are self-certifying and self-managing.

A KERI identifier is abstractly called an Autonomic Identifier (AID) because it is self-certifying and self-managing. A KERI DID is one concrete implementation of a KERI AID. The same KERI prefix may control multiple different DIDs as long as they share the same prefix.



`did:keri:`*`prefix`*`[:`*`options`*`][/`*`path`*`][?`*`query`*`][#`*`fragment`*`]`

`did:keri:ENqFtH6_cfDg8riLZ-GDvDaCKVn6clOJa7ZXXVXSWpRY`

KERI Identifier KEL VDR *Controls* Verifiable Credential Registry TEL VDR

A KERI KEL for a given identifier provides proof of authoritative key state at each event. The events are ordered. This ordering may be used to order transactions on some other VDR such as a Verifiable Credential Registry by attaching anchoring seals to the KEL events.

The set of transactions that determine registry state form a log called a Transaction Event Log (TEL).

Transactions are signed with the authoritative keys determined by the key state in the KEL with the transaction seal.

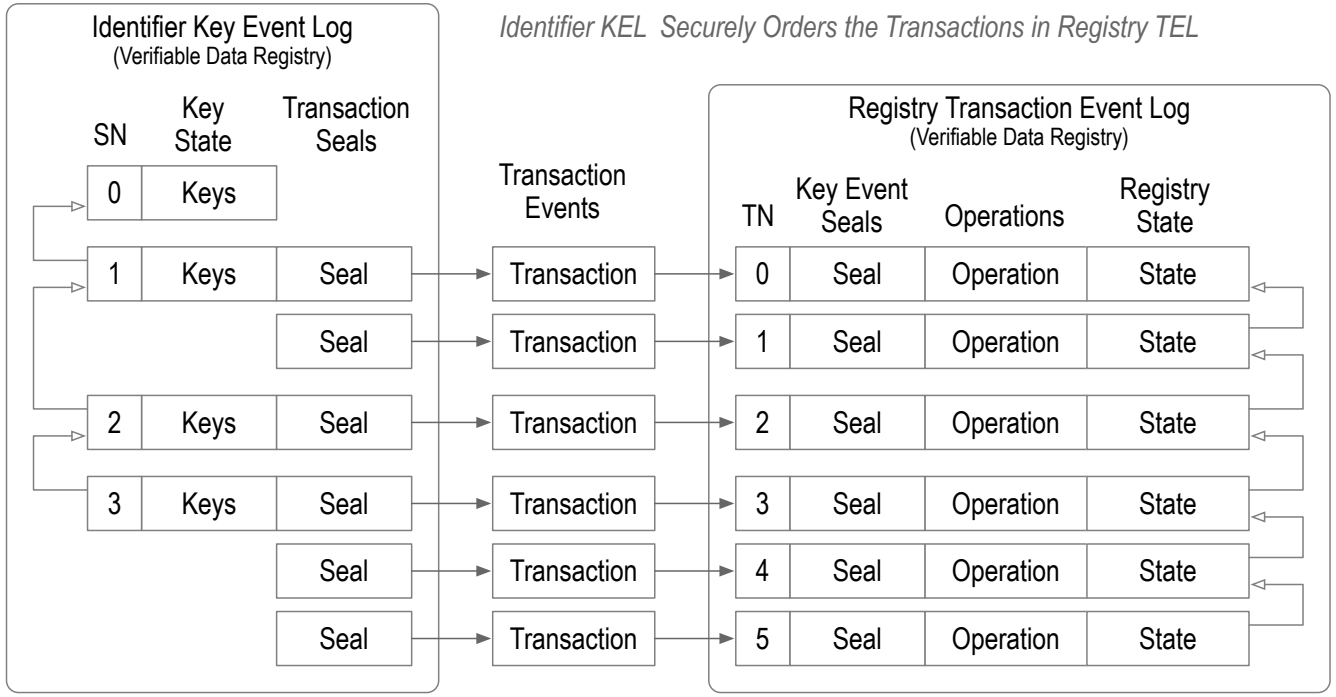
The transactions likewise contain a reference seal back to the key event authorizing the transaction.

This setup enables a KEL to control a TEL for any purpose.

In the case of the vLEI the TEL controls a vLEI issuance and revocation registry.

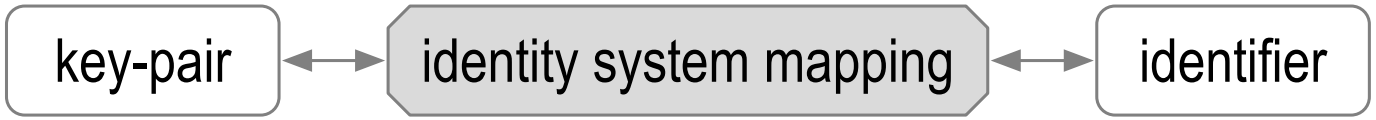
The TEL provides a cryptographic proof of registry state by reference to the corresponding controlling KEL.

Any validator may therefore cryptographically verify the authoritative state of the registry.

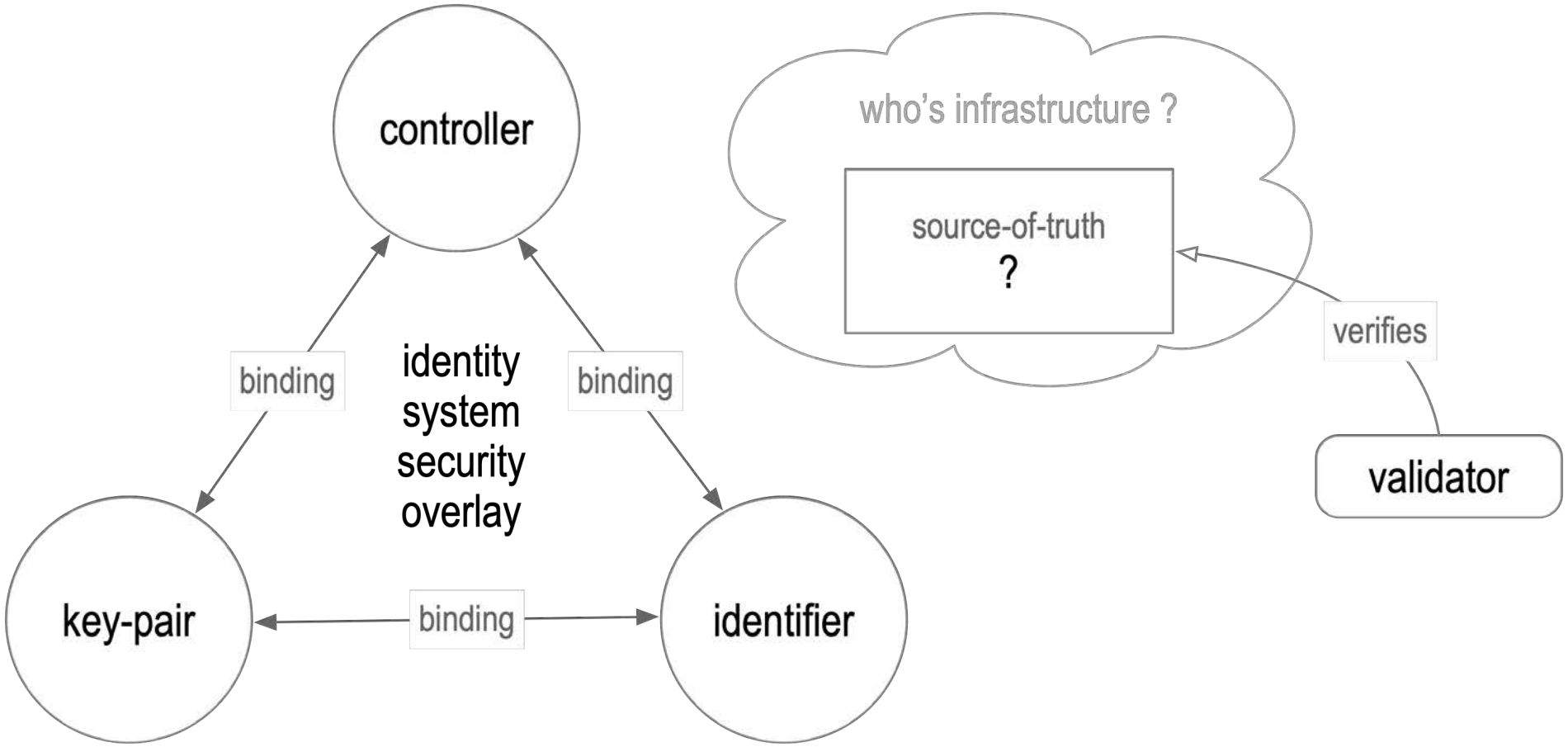


Identifier System Security

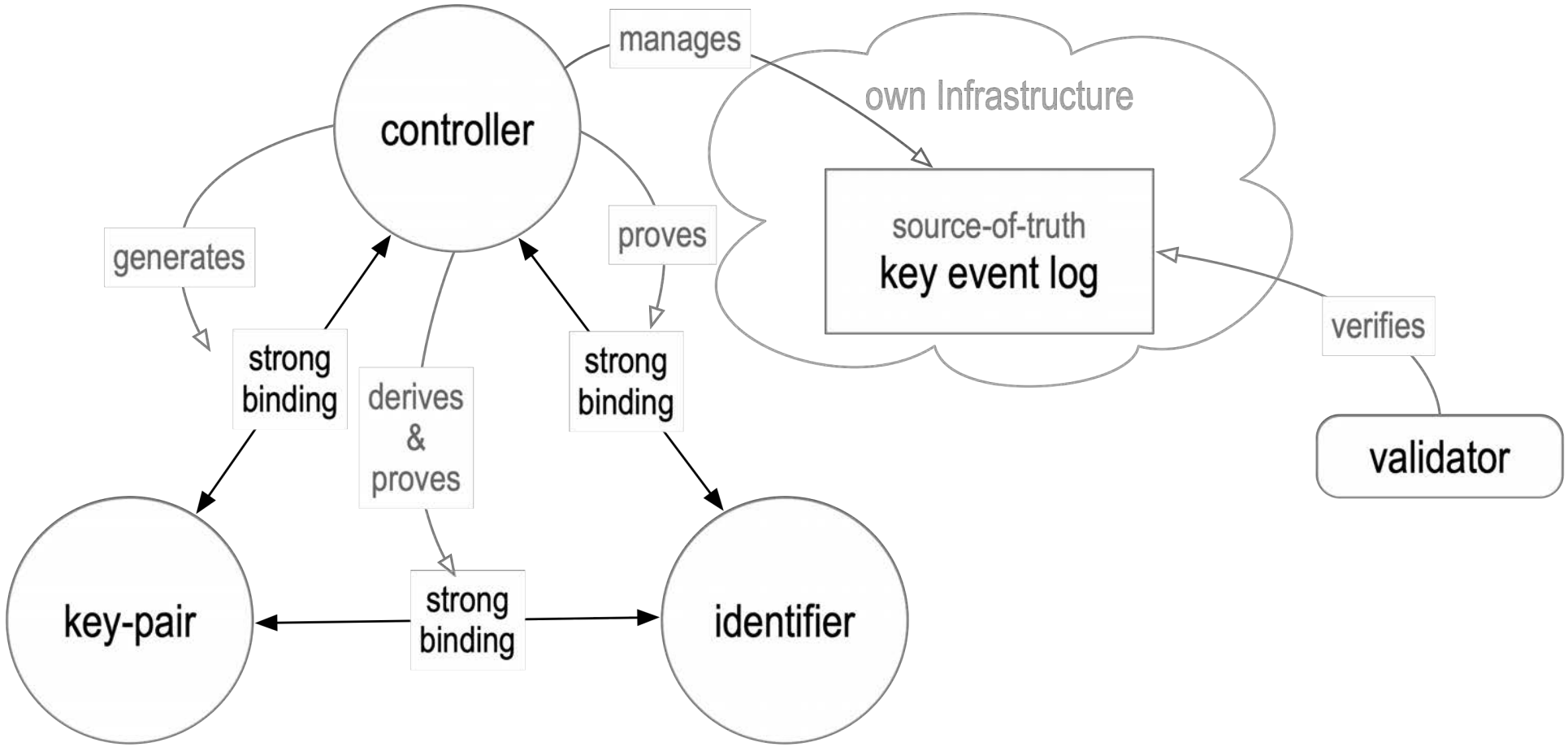
Authentic transmission of data may be verified using an identity system security overlay.
This overlay maps cryptographic key-pairs to identifiers.
When those identifiers are self-certifying they are derived via cryptographic one-way functions from the key pairs.
This provides a self-certifying identifier with a cryptographic root-of-trust.
A key event log (KEL) provide support for secure key rotation without changing the identifier.
Message authenticity is provided by verifying signatures to the authoritative keys pairs for the identifier included in the message.



Trust Basis for Identifier Issuance



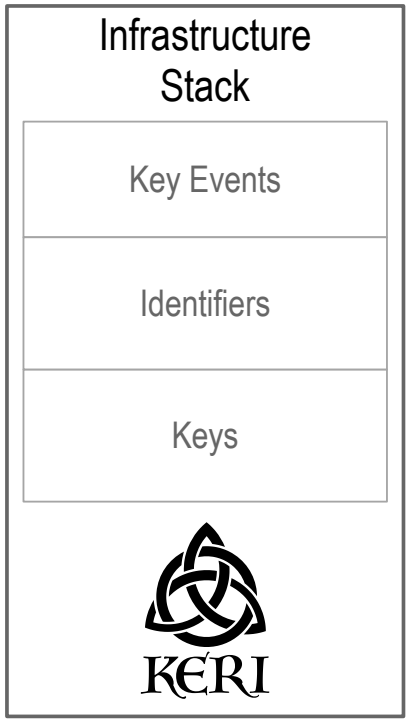
KERI's Autonomic Trust Basis
Cryptographic Root-of-Trust



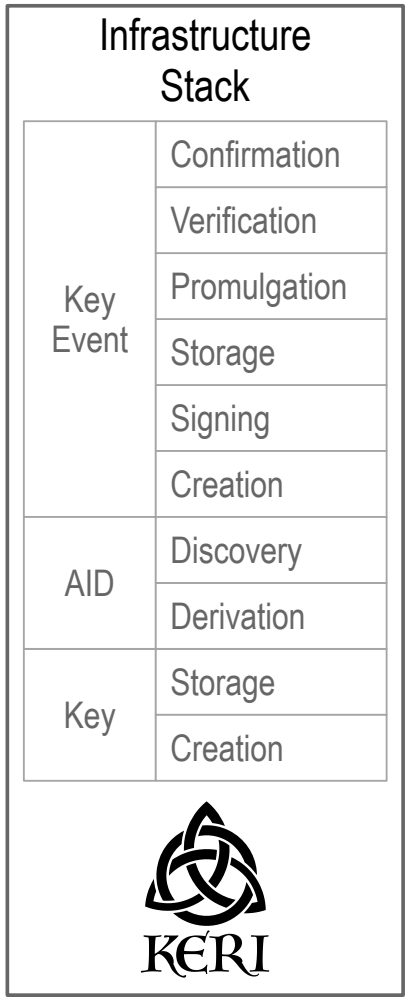
KERI Infrastructure Stack

Support for KERI is provided via open source software running on computing devices.
These constitute the KERI infrastructure stack.
For increased security and scalability, KERI supports delegated identifiers.
Each participant in a delegation may run their own KERI stack.

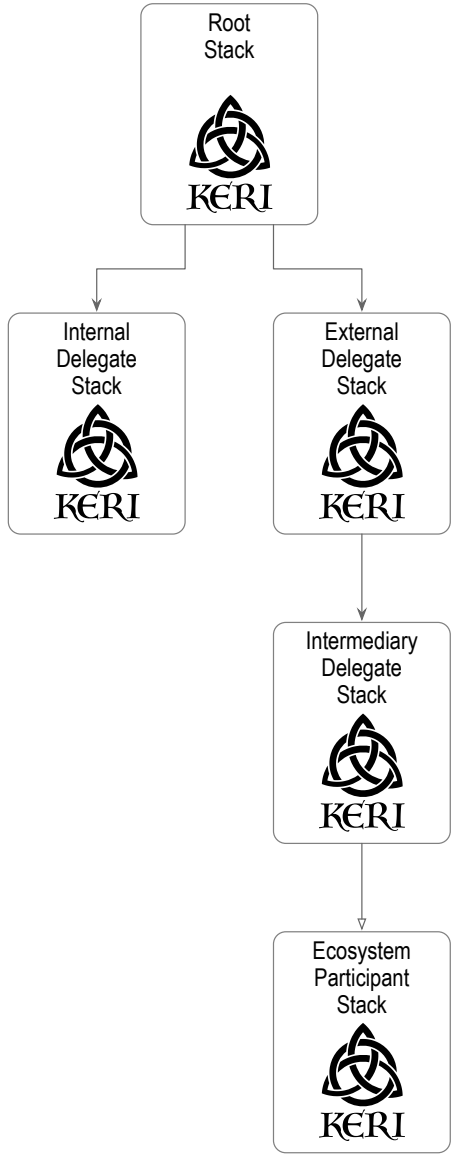
Simple Stack



Detailed Stack



KERI Delegation Stacks



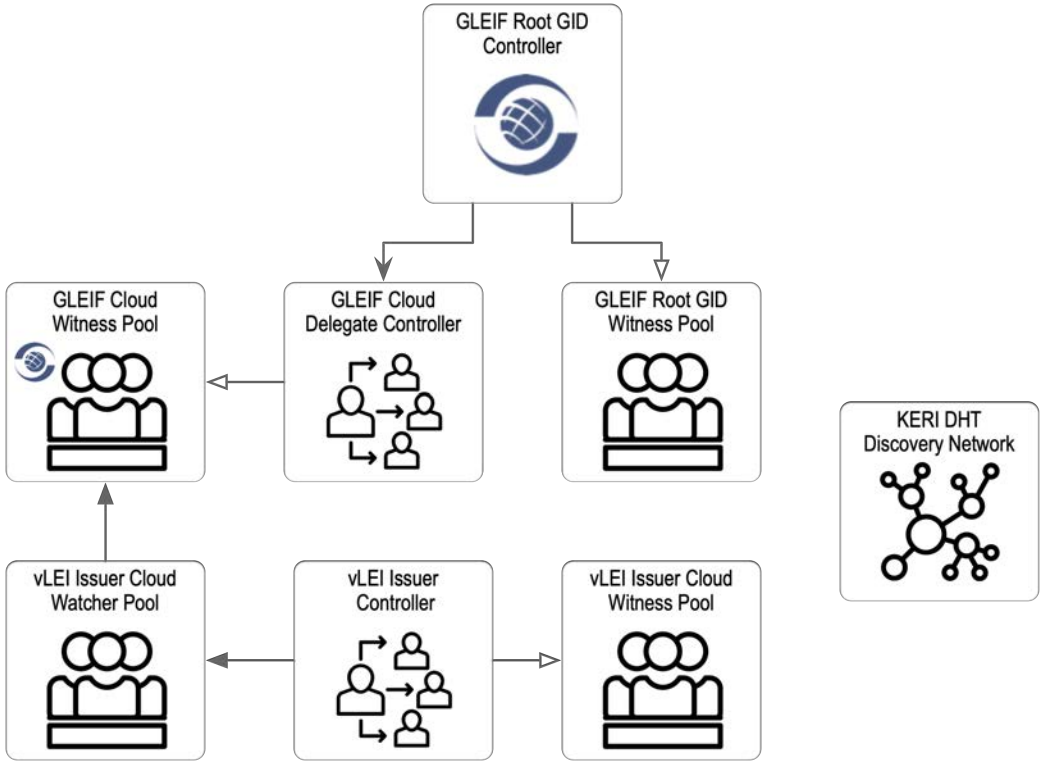
Technical details about the vLEI infrastructure

KERI employs a modular architecture with modular components that each provide services. Participants may configure their stacks to provide some of all of the services or share services provided by others.

The component services include Controller, Witness, Watcher, Delegate, Oracle, Validator.

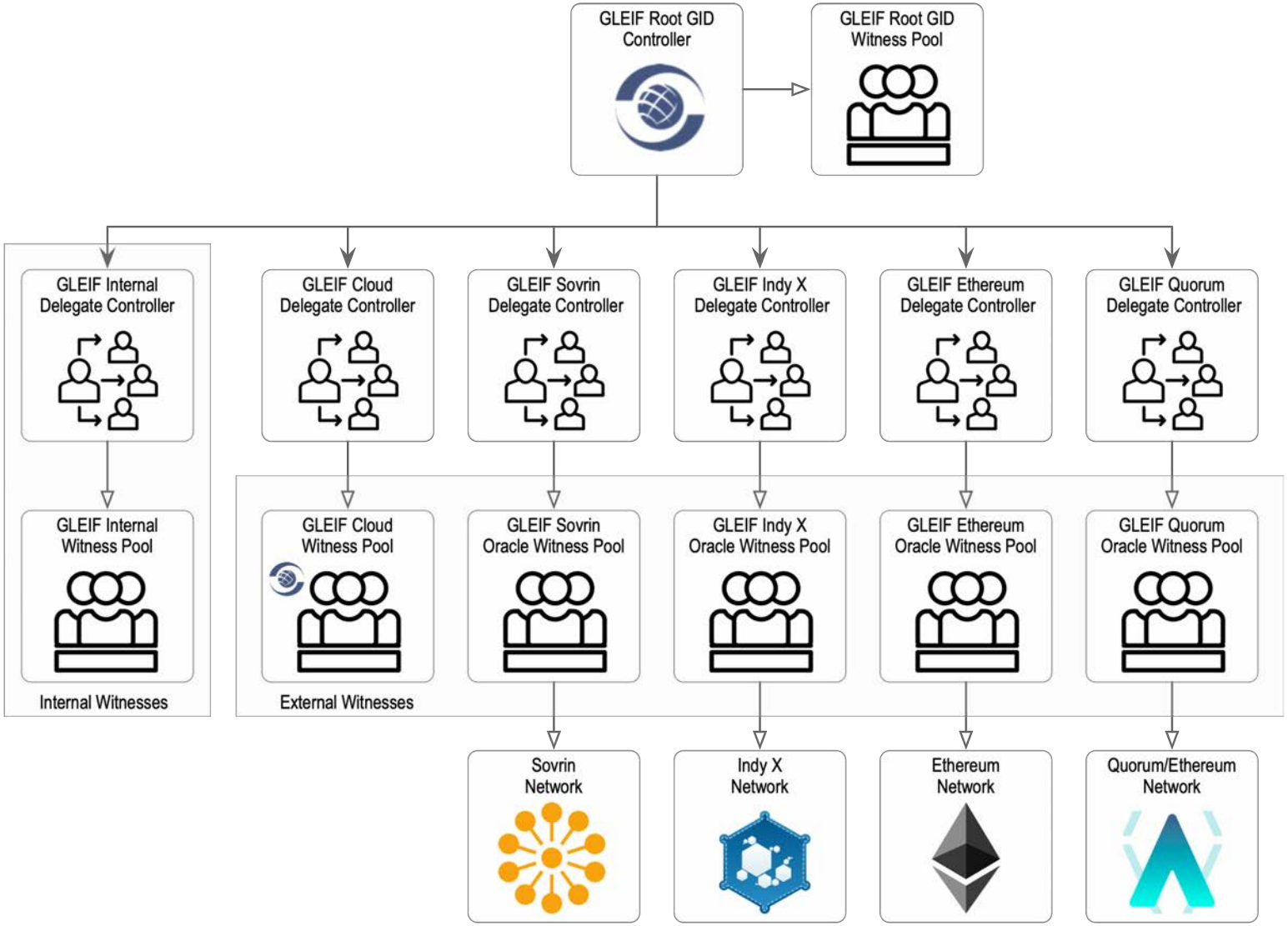
The root-of-trust for the GLEIF ecosystem is provided by a single globally published AID called the GLEIF AID or GID for short. It is a KERI DID.

This GID is the issuer of delegations to other KERI AID DIDs. These delegated identifiers may be the issuers of vLEIs.



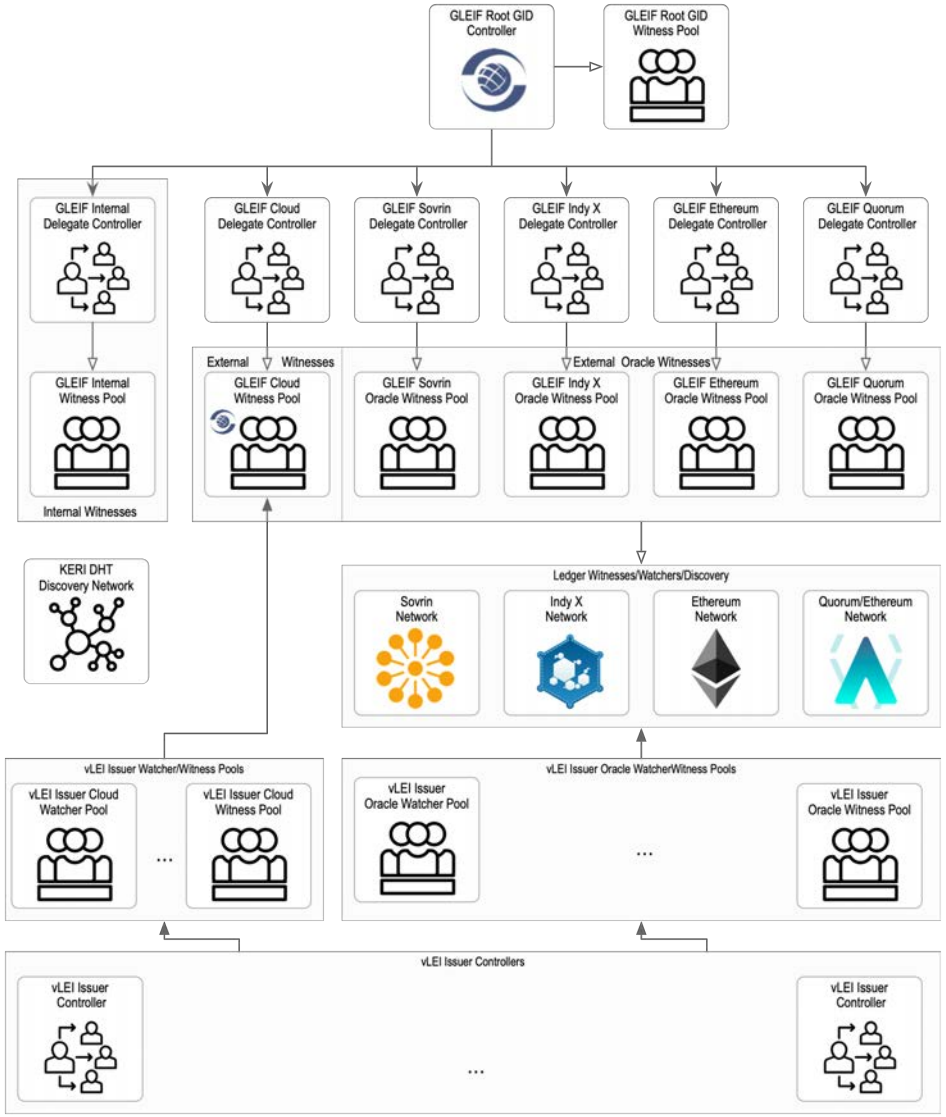
Simplified GLEIF Ecosystem

GLEIF Controller and Witness Network



Components of the GLEIF Ecosystem under GLEIF Control

GLEIF + vLEI Issuer Networks

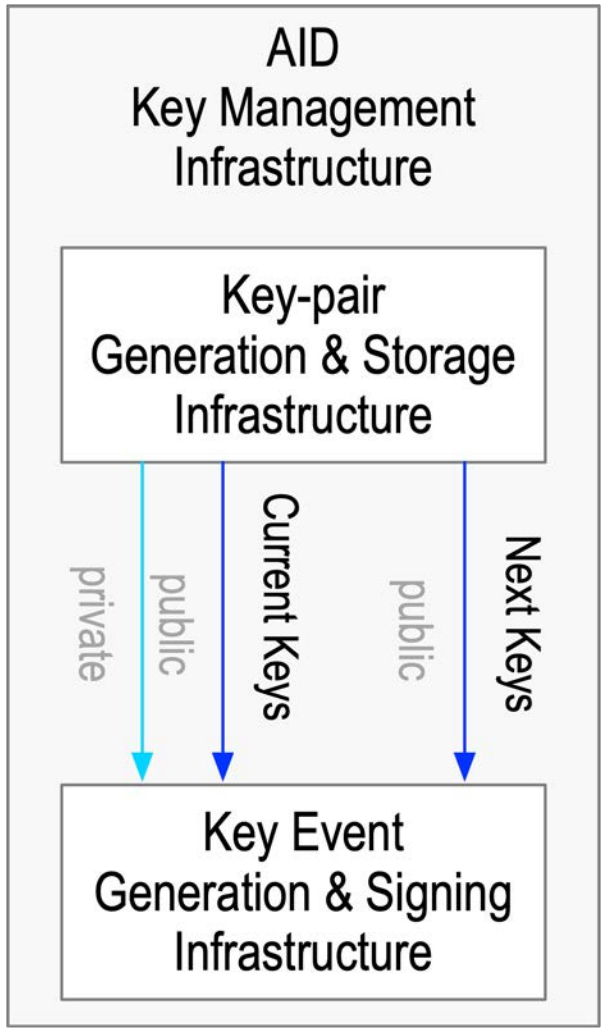


GLEIF Ecosystem with both GLEIF and vLEI issuer controlled components

Decentralized Key Management Infrastructure (DKMI)

KERI's cryptographic trust basis depends primarily on cryptographic key management infrastructure.

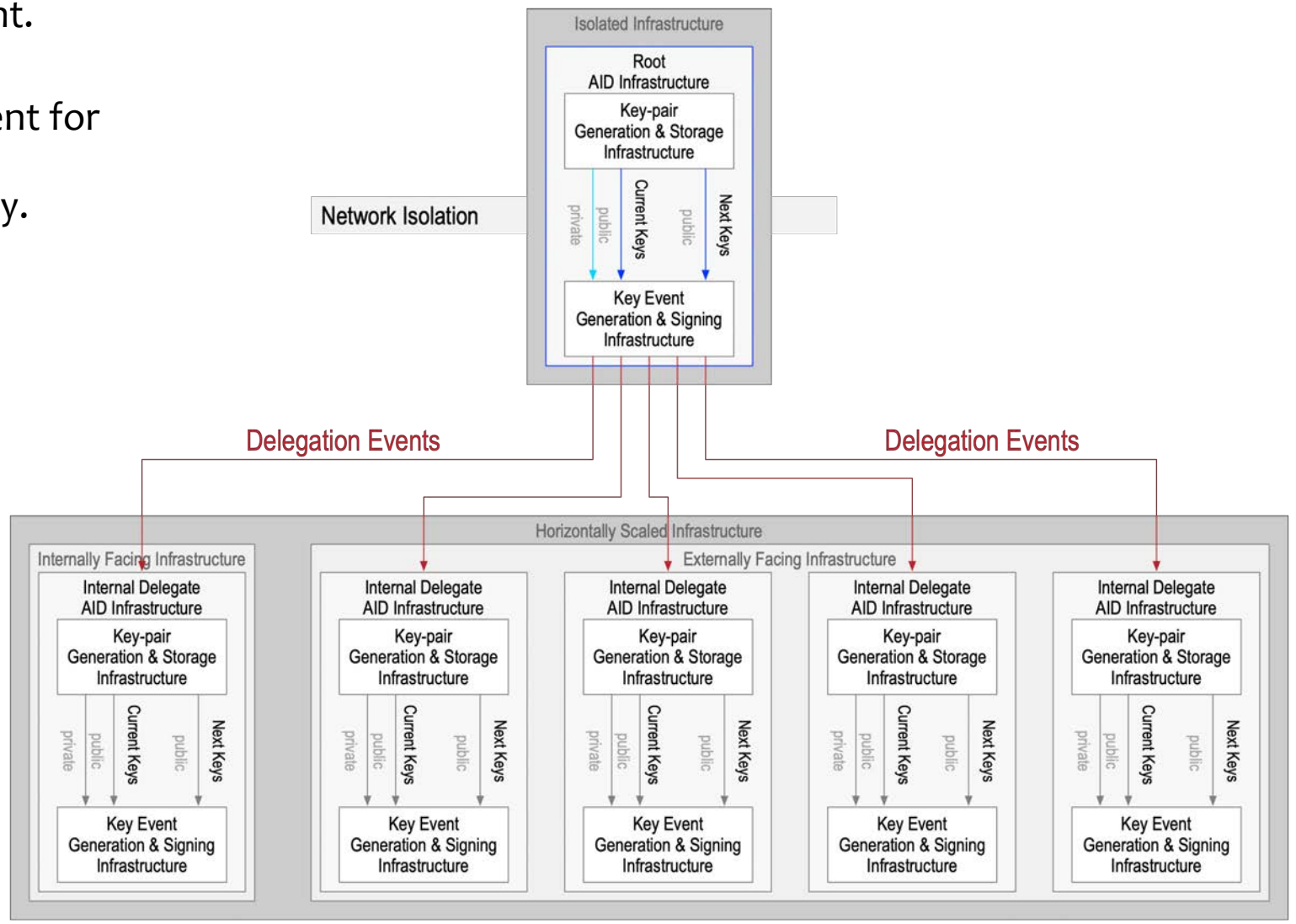
This dependence simplifies security concerns to key management concerns.



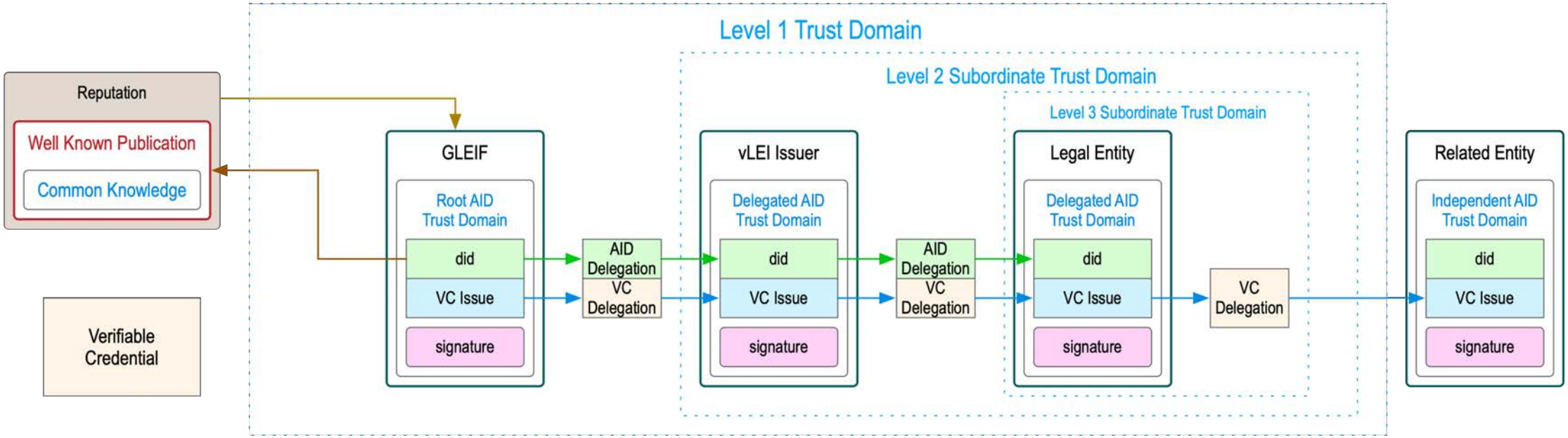
GLEIF Controller Network (DKMI)

KERI supports delegation that enables horizontally scaled key management.

GLEIF's key management for vLEI Issuer identifiers leverages this capability.



GLEIF Ecosystem vLEI Issuance



Each level of delegation forms a nested trust domain that is protected by the level above.
This increases ultimate security while enabling higher performance event issuance in lower layers.

GLEIF's GID provides the root-of-trust for the whole ecosystem. This enables secure decentralized interoperability.

Each trust domain may make delegations of both identifiers and verifiable credentials to a subordinate trust domain. These delegations provide revocable authorizations.

GLEIF Ecosystem VLEI Issuance for Official Organizational Roles and Employees

Delegations may be granular and include authorizations of individual employees. This provides specific scalable but non-repudiable accountability of all participants in the eco-system.