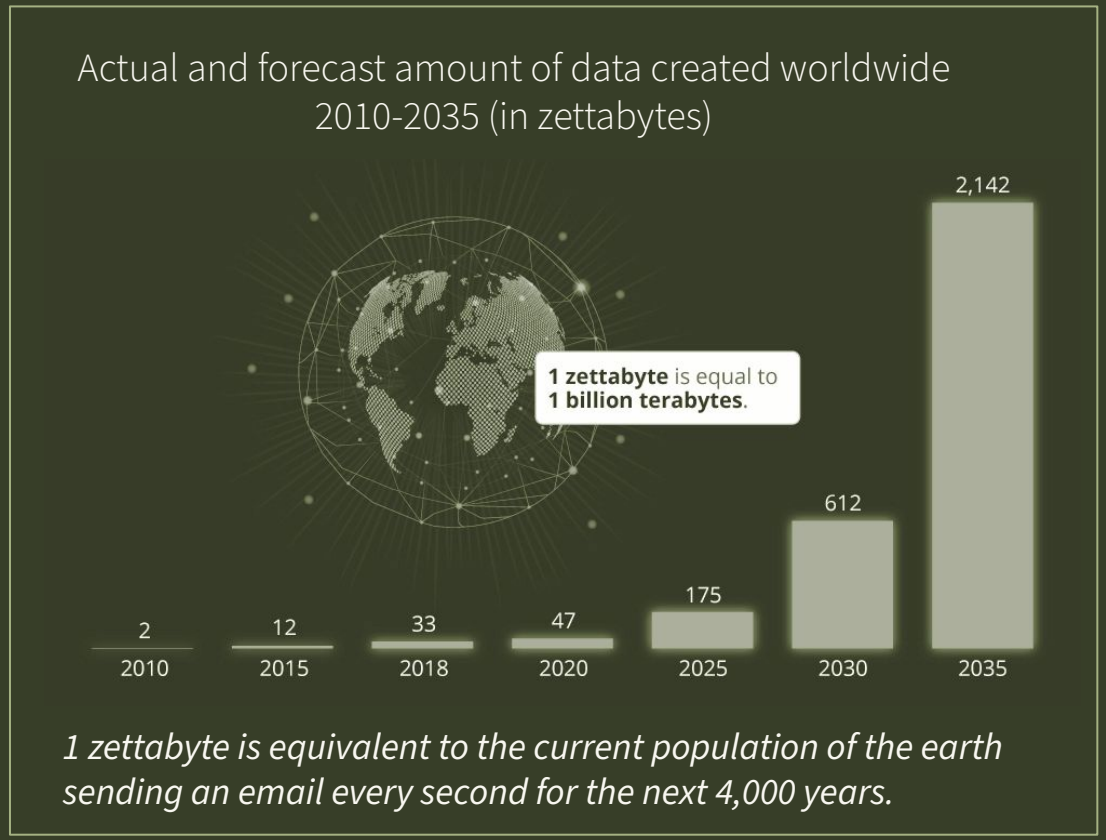
and Key

How I learned to stop worrying and love the log

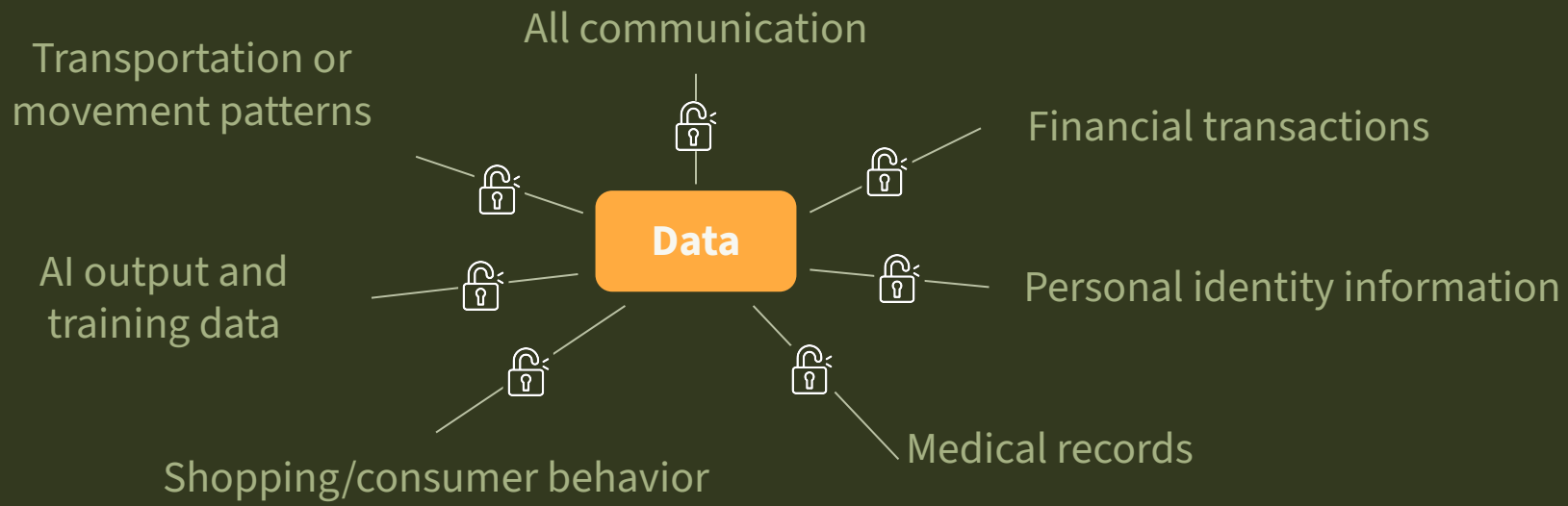
Where are we?



In 2025, **175 Zettabytes of data** will be created

There is currently **no way to make any of it globally verifiable data**

There is currently no way to create globally verifiable data in a truly secure way



Cybercrime will cost the world 1 trillion USD per month by 2031

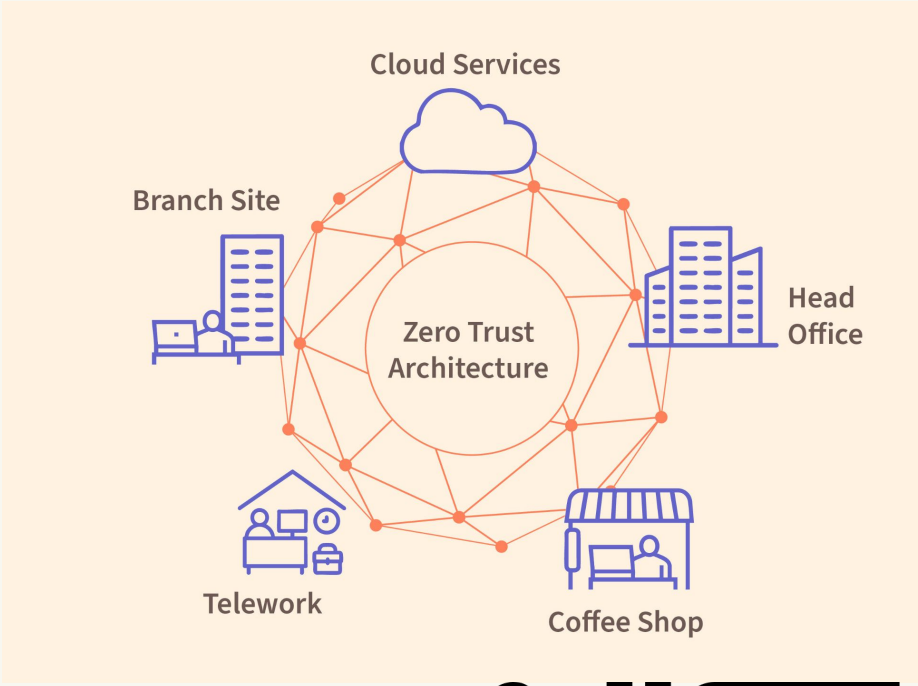
According to cybersecurity ventures cyber report 2025, global cyber crime course to grow by 15% over the next 2 years reaching $10.5 trillion USD annually by 2025 and $ 12 trillion USD in 2031 up from 3 trillion from 2015.

Global Fraud: $10.5 trillion USD annually by 2025 and **$12 trillion USD in 2031**

Information (therefore value) chains are in crisis

Zero Trust, Verify

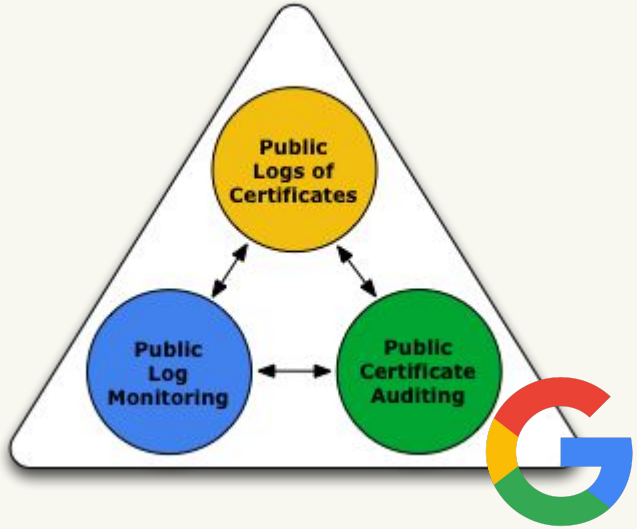
- NIST publication SP 800-207
- Presumes (eventual) key compromise, instead of the traditional “castle moat” approach to cyber security
- Motivated in response to Project Aurora, massive cyber attack purported by Chinese state sponsored blackhats after 2008
- Powerful in promoting cybersecurity from first principles, but can promote operational bloat, cost, and UX friction



NIST

Certificate Transparency

- Break of DigiNotar in 2011 for (what else) state actor malfeasance.
- Google developers led adaptation
- Problems with trustless key discovery and fork prevention
- Working toward the steeling of PKI infrastructure against current and future efforts



Insecure Key exchanges & shared secrets are **everywhere**

Enter KERI

KEY EVENT RECEIPT INFRASTRUCTURE (KERI) DESIGN [1][2]

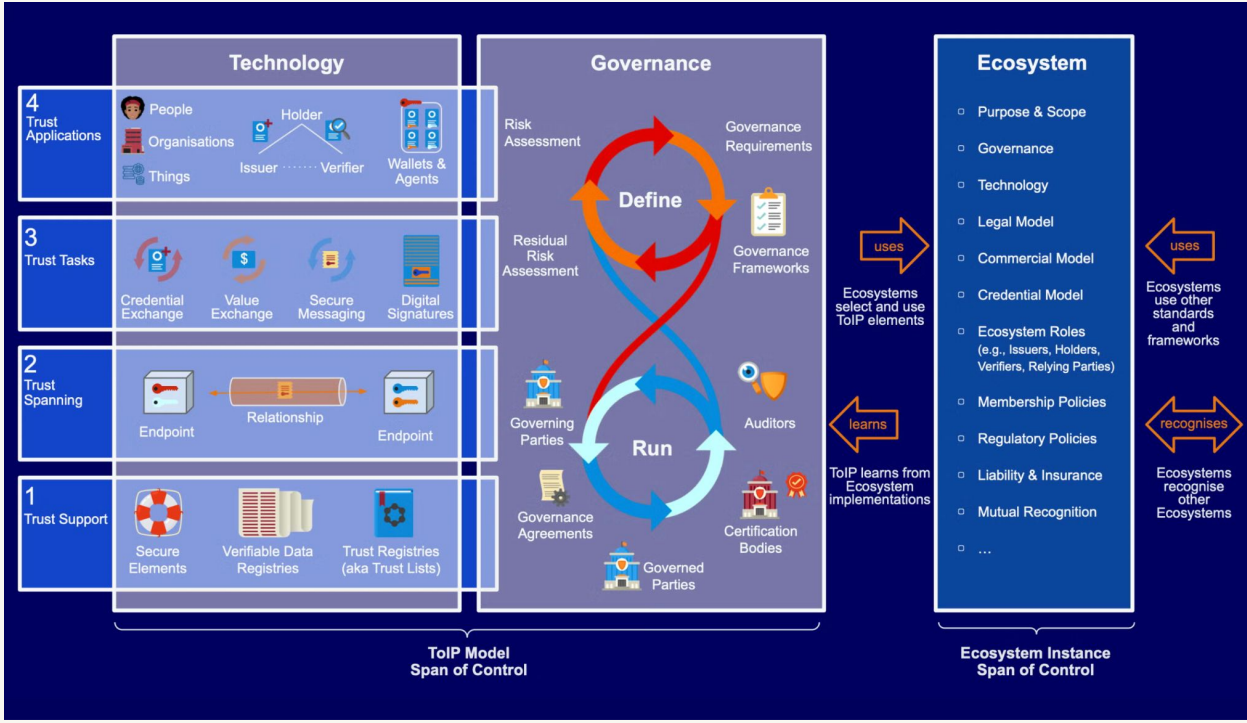
Samuel M. Smith, Ph.D.

v2.63 2025/09/14, original 2019/07/03

Abstract—An identity system-based secure overlay for the Internet is presented. This includes a primary root-of-trust in self-certifying identifiers. It presents a formalism for Autonomic Identifiers (AIDs) and Autonomic Namespaces (ANs). They are part of an Autonomic Identity System (AIS). This system uses the design principle of minimally sufficient means to provide a candidate trust-spanning layer for the internet. Associated with this system is a decentralized key management infrastructure (DKMI). The primary root-of-trust are self-certifying identifiers that are strongly bound at issuance to a cryptographic signing (public, private) key-pair(s). These are self-contained until/unless control needs to be transferred to a new key-pair. In that event, an append-only chained key-event log of signed transfer statements provides end-verifiable control provenance. This makes intervening operational infrastructure replaceable because the event logs may be served up by any infrastructure, including ambient infrastructure. End-verifiable logs on ambient infrastructure enable ambient verifiability (verifiable by anyone, anywhere, at any time).

History

- Occupies the layers 1-3 in the Governance Framework
- Bounced around the ecosystem until finding its home in Trust Over IP
- Chosen by GLEIF to host their “verifiable LEI”

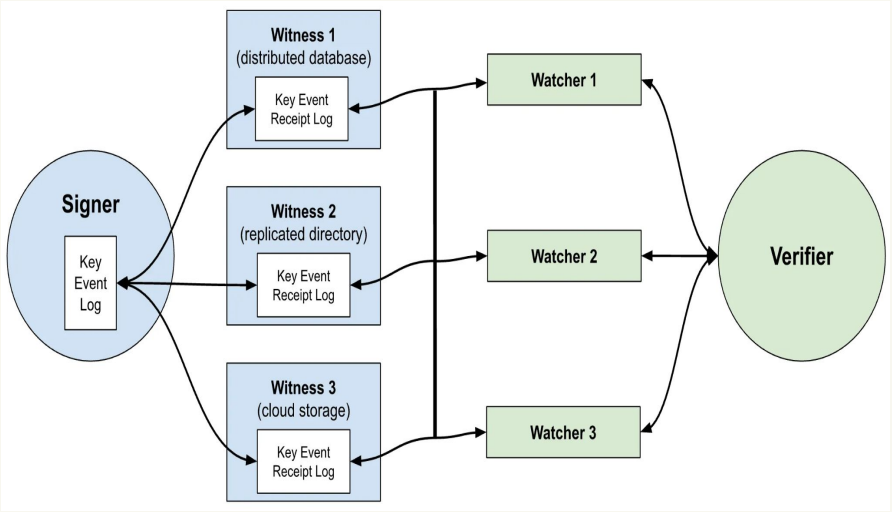


Roots in the Chain

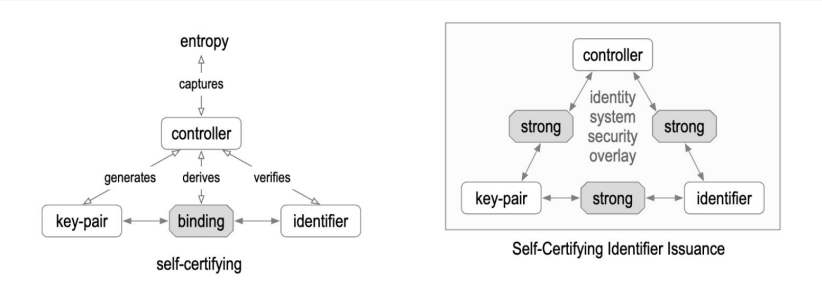
Principles come from classic blockchains, but..

- The consensus is driven by key holder (signer)
- Separation of signing and verifying

  infrastructure (watchers and witnesses)
- Duplicity detection (of the identifier) is baked into the architecture



Src: https://rufftimo.medium.com/keri-101-witnesses-watchers-detectability-fb604cae7a26



Src:KERI Whitepaper

Roots in the Chain *(cont.)*

- Pre-Rotation+Key Event Logs allow for permanent term identifiers and perpetual control.
- Content addressable chained data containers (SAIDs+ACDCs) embedded in the chain of trust allow for contextual determination of access control

ALL THIS LEADS TO.....

A PKI system an order of magnitude more
Secure *and* **Simple**

Three Main Primitives

- Inception (ICP)- Creates the identifier at Sequence 0, distributed to all witness nodes
- Interaction (IXN)- Records non-Key State changes like credential anchoring, registry creation, delegation, and revocation
- Rotation (ROT)- Rotates to the pre-committed, blinded key sealed in the inception event's "n" field

These primitives serve as the minimal "instruction set" for creating decentralized trust ecosystems.

Globally resolvable **KEY STATE**

For the first time in history a person or thing can:

Retrieve the **Key State** (the current state of a cryptographic key) tied to a cryptographic identifier (vLEI)

without the use of identity providers (IDPs), blockchains, or shared platforms,

with the ability to **fully recover** from compromise,

Without having to use **a new identifier to recover.**

KERI Suite

- ACDC (Authentic Chained Data Container) Task Force
- DID WebS Method Task Force
- SAID URN Charter Task Force
- Dossier Implementation Guide Task Force

KERI Suite WG Deliverables

- KERI Spec
- ACDC Spec
  - (Authentic Chained Data Containers)
  - Serves as the technical basis for implementing “Digital Dossiers”
- CESR Spec
  - (Composable Event Streaming Representation)
  - Serves as the basis of inspiration for the Trust Spanning Protocol
- did:webs Spec
  - DID method which uses traditional web infrastructure in order to publish DIDs, but not rooted in traditional certificate authorities

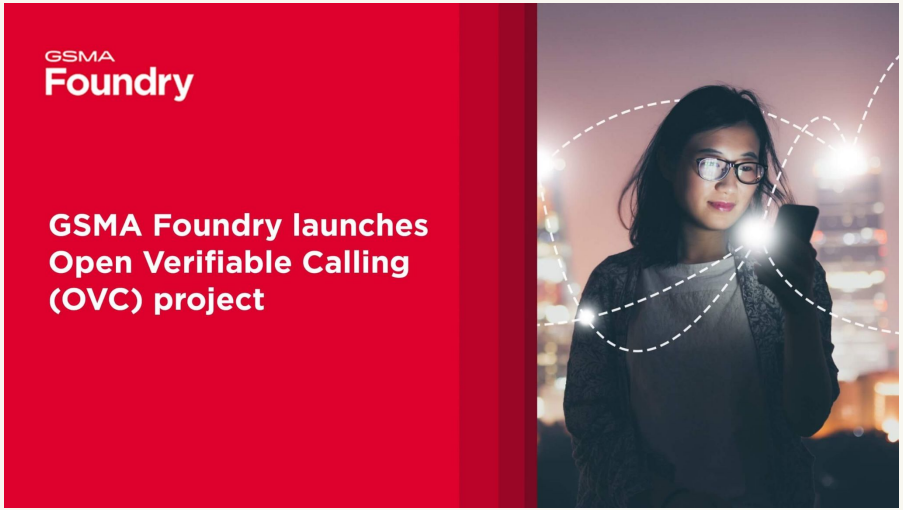
Finally, adoption!

SEDI as major catalyst

- **S**tate **E**ndorsed **D**igital **I**dentity
- Filling in the empty space around the technical implementations
- Constitutionally derived Legal Framework
- Purports to be the solution to the “No Phone Home”
- Critical questions such as digital delgatability
- Seeks to build a consortia of other states building digital identity from first principles via the SEDI Consortium

Open Verifiable Calling

- Global PoC hosted by the GSMA Foundry
- Goal of cryptographically verifying origination of calls and scaling branded calling
- Based upon the work of Daniel Hardman (inventor of DIDCOMM, Chief Architect of Provenant), Verifiable Voice Protocol.
- GSMA will adapt the Governance Framework from GLEIF (vLEI) to build their own trust fabric.



PROVENANT
verifiable communications

HealthKERI in Techstars

- Great validation of a business model built on open source software
- 1-2% of applications make it through!
- Key Strategic hub (Medtech center of America)
- Looking to secure healthcare data exchange across America, watch this space!

ARCHIMEDES

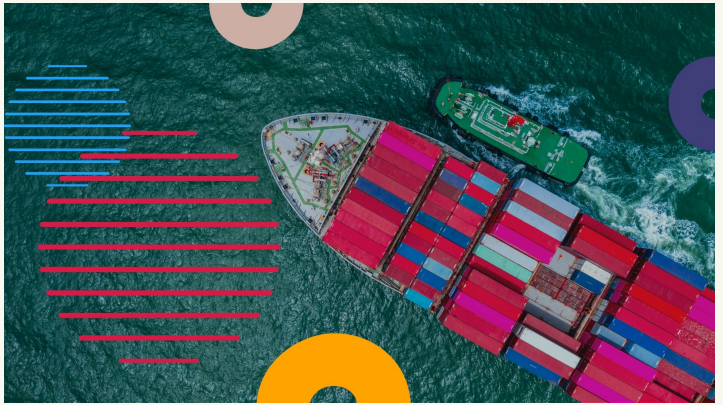
KEY STATE CAPITAL

vLEI Hackathon

- 3 Locations (New York, Frankfurt, Hong Kong)
- 3 Themes (Finance, SME Finance, Industry)
- **London Stock Exchange Group** won the Finance branch, with full asset lifecycle modeling with vLEI as a root
- **Dataswyft** won the SME Finance branch, with a seamless onboarding process for the end-user to leverage their vLEI to onboard into credit markets
- Final Event to occur in Frankfurt on Dec 2nd, see you there!

Verifiable.Trade

- Founded by former CEO of GLEIF, Stephan Wolf
- Uniquely focused on making trade interoperable across different platforms, via the ISTTP Protocol
- Influencing discussion around best practices alongside the UNTP (United Nations Trust Protocol), ICC DSI, ML-ETR, and ML-IT standards.
- ISTTP//: is still at early stage, but promises to bring Zero Trust to supply chains around the world



A Growing Ecosystem

GSMA™

PROVENANT

Microsoft

Dowsers

Switchchord

esatus

Verifiable.Trade

TM

accelerate
caring minds

healthKERI

Cardano
Foundation

KEY STATE CAPITAL

PSICURITY™

ISO

What's next

- More:
  - Developers
  - Founders
  - Roots of Trust (and therefore…)
  - Industries
  - Companies, companies, companies!
- An ecosystem of governance frameworks
- Further refinements to the KERI suite
  - OC-SMT
  - Reliable UDP delivery
  - 5Ws (Wallets, Watchers, Witnesses, **Wizards**, Web)
  - Interoperability/Acceptance modes
- Finalizing the implementation of SPAC

vLEI – The Rise of Organizational Identity

This report explores how vLEI can solve systemic identity challenges, like fragmented registries and analog verification, by enabling cryptographically verifiable, decentralized organizational identity at scale.

With 9 different use cases, it positions vLEI as critical infrastructure for trusted, automated business interactions. →

vLEI on-chain:
Verifiable Smart Contracts

This report explores how KERI, as the method of cryptographic attestation, can connect organizational identity with on-chain smart contracts, thereby bringing compliance directly into contact with Web3 infrastructure

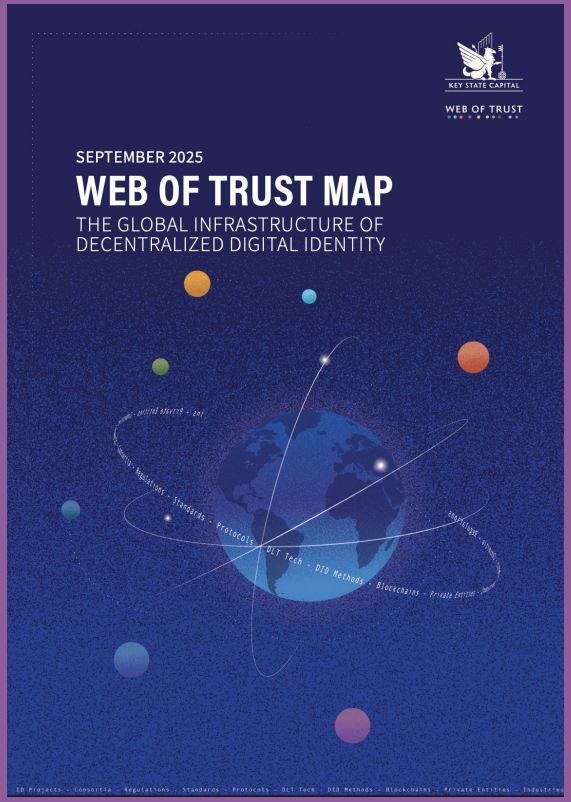
This is more than just a high-level theory; we include direct technical direction as to how you can achieve this groundbreaking interoperability. See how! →

KEY STATE CAPITAL

Web of Trust Map:
The Global Infrastructure of Decentralized Digital Identity

If you haven't seen, please take a look at the our visual of the entire digital identity space: the Web of Trust Map!

Our research has yielded incredible results, with 30+ Industries, 260+ Projects, and contributions from over a dozen digital identity experts. This is truly a must see for anyone interested in the future of our digital space →



KEY STATE CAPITAL

vLEI.wiki

The Verifiable Legal Entity Identifier & KERI Knowledge Base

Turn your AI assistant into a KERI/vLEI expert: get the MCP

Search concepts and source documents... Search

437 Key Concepts **3650** Source Documents **463** Glossary Terms Generated from GitHub sources

About vLEI.wiki

vLEI.wiki is a knowledge base designed for AI agents and technical practitioners working with the vLEI/KERI protocol and ecosystem, made by Key State Capital. Our content is specifically optimized for consumption via the **Model Context Protocol (MCP)**, enabling seamless integration with AI tools like Claude Desktop, Cursor, and VS Code. This enables AI coding assistants to help with vLEI/KERI development and research at an expert level. API keys are free to all users and available here.

vLEI.wiki indexes all published vLEI/KERI documentation and provides comprehensive AI generated summaries and explanations of key terms and concepts in the vLEI/KERI ecosystem. Each concept is generated from multiple source documents and includes detailed technical explanations, implementation notes, and connections to related topics.

Thank you!

- This community is only possible via the passion of dozens of developers, executives, thought leaders, public servants and investors in the space
- Your time and energy is the lifeblood of our movement, it is greatly appreciated.

Join us in the KERI Suite WG meetings, if you want to learn more!