Key Event Receipt Infrastructure

A Trust Spanning Layer for the Internet

https://keri.one

Samuel M. Smith Ph.D. Senior Member IEEE

sam@prosapien.com

IEEE Virtual Event BlockChain Session 2

2021/10/21

Resources

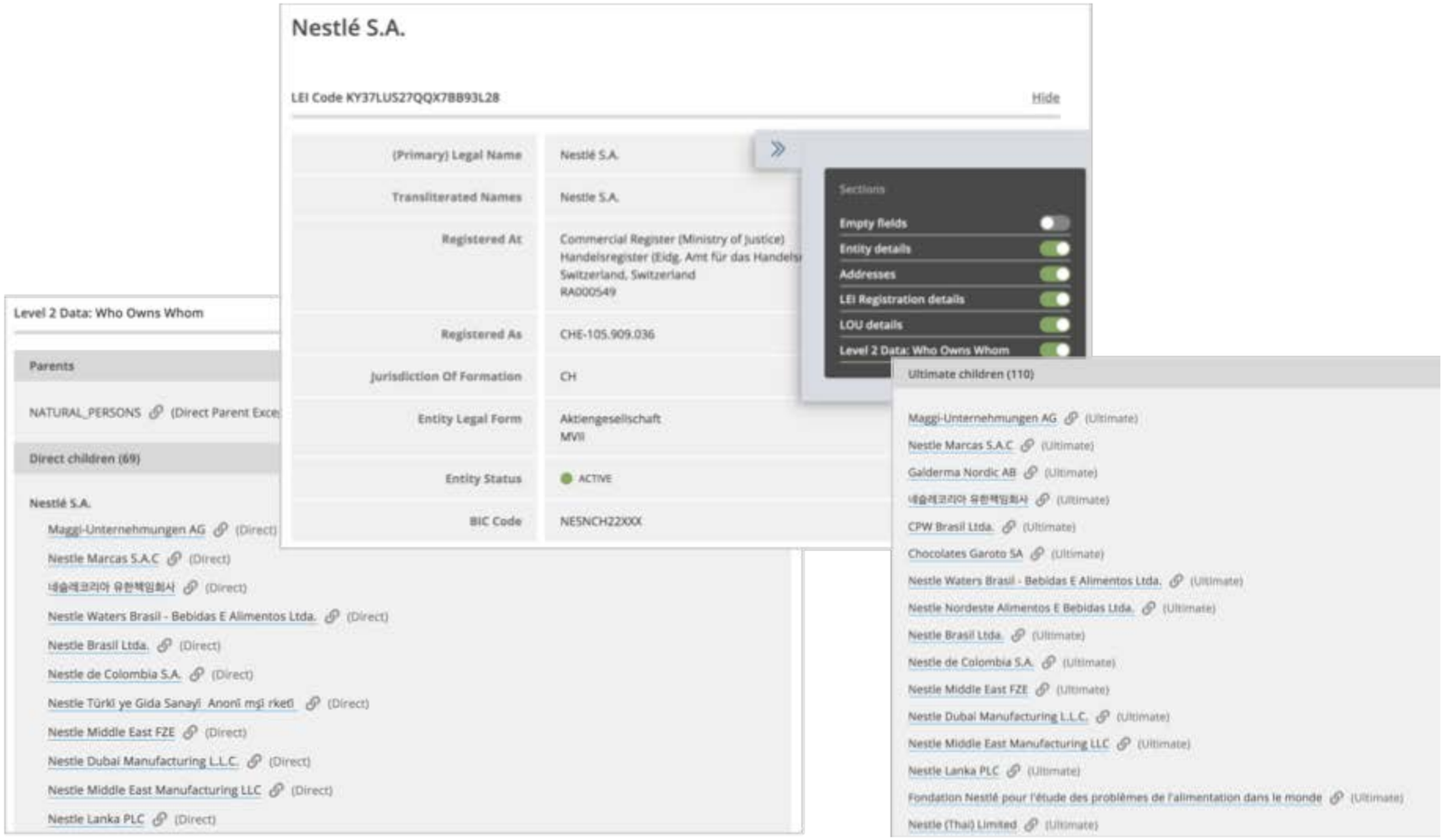
Documentation:
https://keri.one/keri-resources/
https://arxiv.org/abs/1907.02143 (KERI White Paper)

Community: (meetings, open source code, IETF internet drafts)
https://github.com/WebOfTrust
https://github.com/WebOfTrust/keri

GLEIF:
https://www.gleif.org/en/lei-solutions/gleifs-digital-strategy-for-the-lei/introducing-the-verifiable-lei-vlei

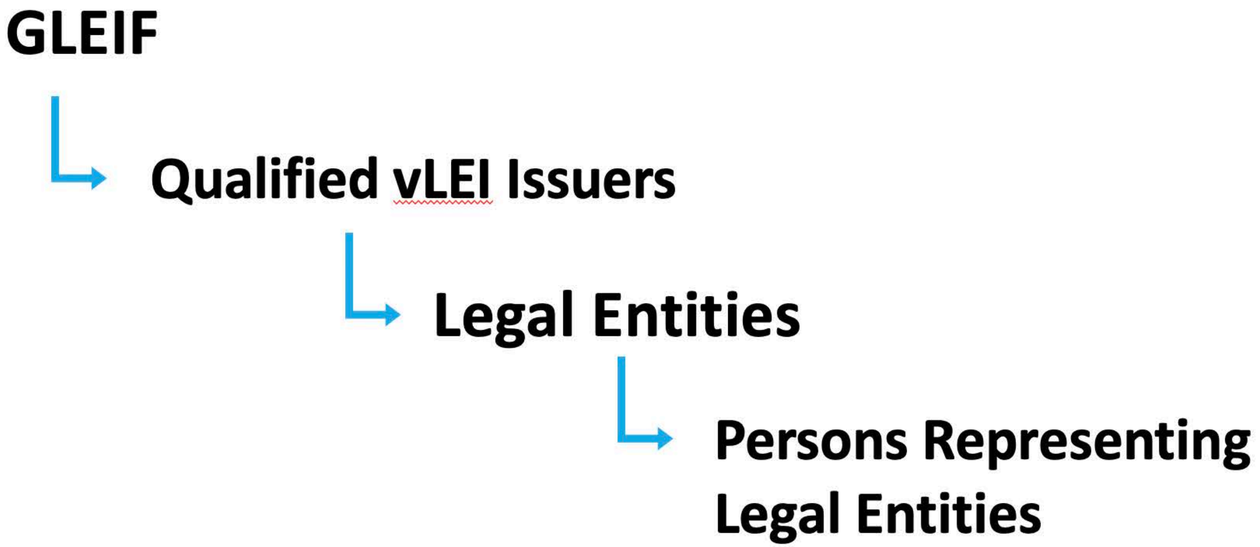
The Legal Entity Identifier – the LEI

- The LEI is a life-long code **owned** by the respective legal entity.
- It points to the associated reference data.
- The LEI is an ISO standard ISO 17442



The LEI as a Verifiable Credential – the vLEI Trust Chain

- Every verifiable LEI (vLEI) is created by an **issuer**
- The issuer **cryptographically** signs the credential with its private key
- An issuer is the organization or entity that asserts information about a **subject** to which a credential is issued
- The vLEI Issuer is an organization **qualified** by GLEIF as part of a trusted network of partners
- GLEIF issues vLEIs to Qualified vLEI Issuers as attestation of trust.
- GLEIF is the Root of Trust



Background References

Self-Certifying Identifiers:

Girault, M., "Self-certified public keys," EUROCRYPT 1991: Advances in Cryptology, pp. 490-497, 1991
https://link.springer.com/content/pdf/10.1007%2F3-540-46416-6_42.pdf

Mazieres, D. and Kaashoek, M. F., "Escaping the Evils of Centralized Control with self-certifying pathnames," MIT Laboratory for Computer Science,
http://www.sigops.org/ew-history/1998/papers/mazieres.ps

Kaminsky, M. and Banks, E., "SFS-HTTP: Securing the Web with Self-Certifying URLs," MIT, 1999
https://pdos.csail.mit.edu/~kaminsky/sfs-http.ps

Mazieres, D., "Self-certifying File System," MIT Ph.D. Dissertation, 2000/06/01
https://pdos.csail.mit.edu/~ericp/doc/sfs-thesis.ps

TCG, "Implicit Identity Based Device Attestation," Trusted Computing Group, vol. Version 1.0, 2018/03/05
https://trustedcomputinggroup.org/wp-content/uploads/TCG-DICE-Arch-Implicit-Identity-Based-Device-Attestation-v1-rev93.pdf

Autonomic Identifiers:

Smith, S. M., "Open Reputation Framework," vol. Version 1.2, 2015/05/13
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/open-reputation-low-level-whitepaper.pdf

Smith, S. M. and Khovratovich, D., "Identity System Essentials," 2016/03/29
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/Identity-System-Essentials.pdf

Smith, S. M., "Decentralized Autonomic Data (DAD) and the three R's of Key Management," Rebooting the Web of Trust RWOT 6, Spring 2018
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/DecentralizedAutonomicData.pdf

Smith, S. M., "Key Event Receipt Infrastructure (KERI) Design and Build", arXiv, 2019/07/03 revised 2021
https://arxiv.org/abs/1907.02143

Smith, S. M., "Key Event Receipt Infrastructure (KERI) Design", 2019-2021
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

Stocker, C., Smith, S. and Caballero, J., "Quantum Secure DIDs," RWOT10, 2020/07/09
https://github.com/WebOfTrustInfo/rwot10-buenosaires/blob/master/final-documents/quantum-secure-dids.pdf

Smith, S. M., "Universal Identifier Theory", 2020/10/23
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/IdentifierTheory_web.pdf

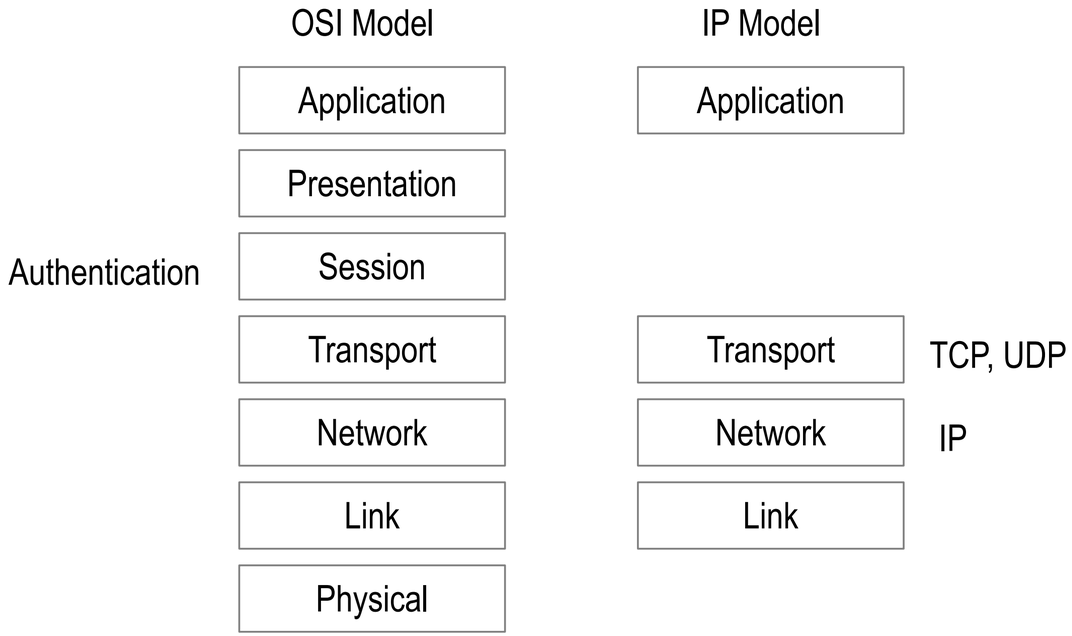
Certificate Transparency:

Laurie, B., "Certificate Transparency: Public, verifiable, append-only logs," ACMQueue, vol. Vol 12, Issue 9, 2014/09/08
https://queue.acm.org/detail.cfm?id=2668154

Google, "Certificate Transparency,"
http://www.certificate-transparency.org/home

Laurie, B. and Kasper, E., "Revocation Transparency,"
https://www.links.org/files/RevocationTransparency.pdf

The Internet Protocol (IP) is *bro-ken* because it has no *security* layer.



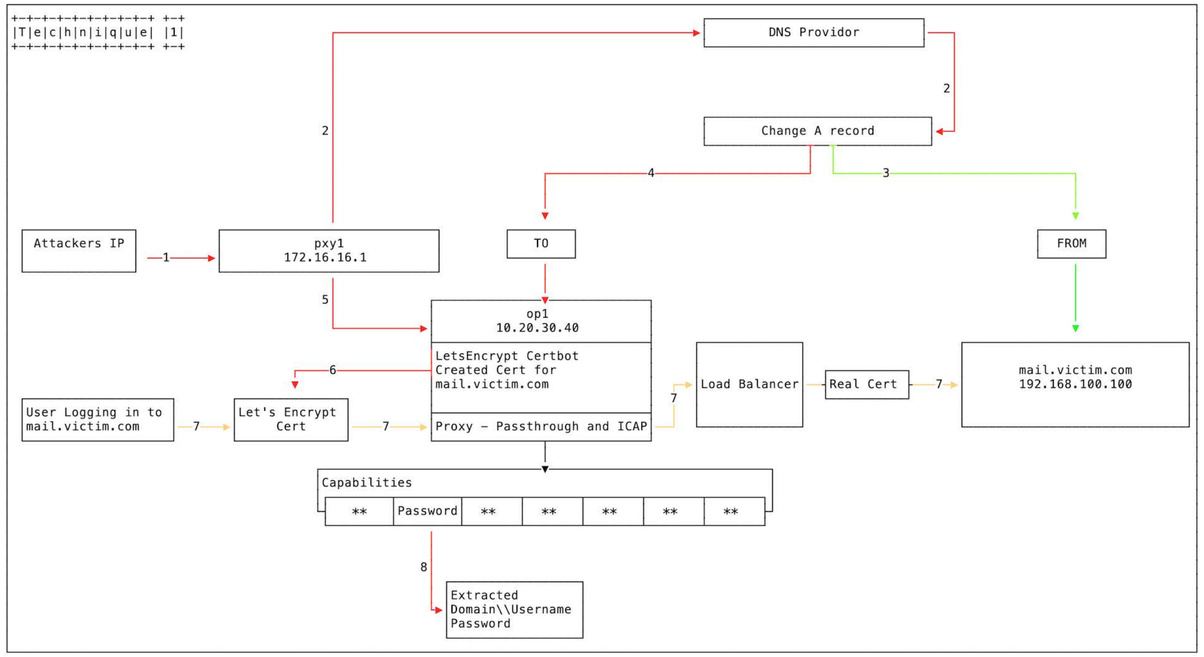
Instead …

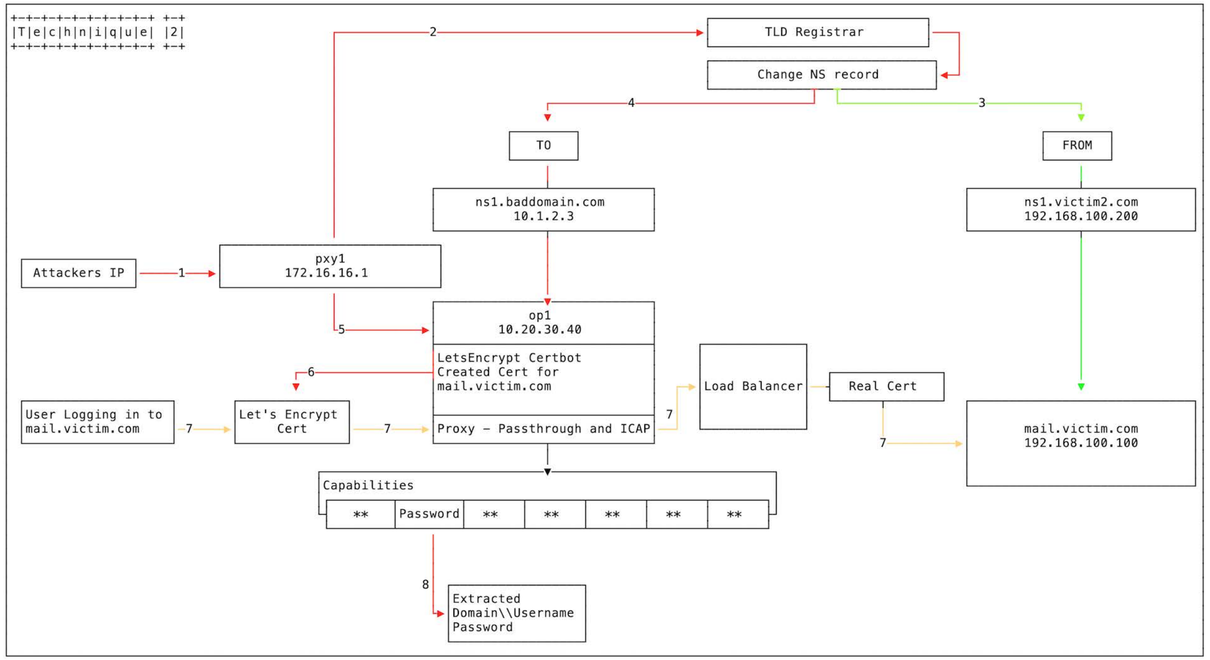
We use *bolt-on* identity system security overlays. (DNS-CA …)

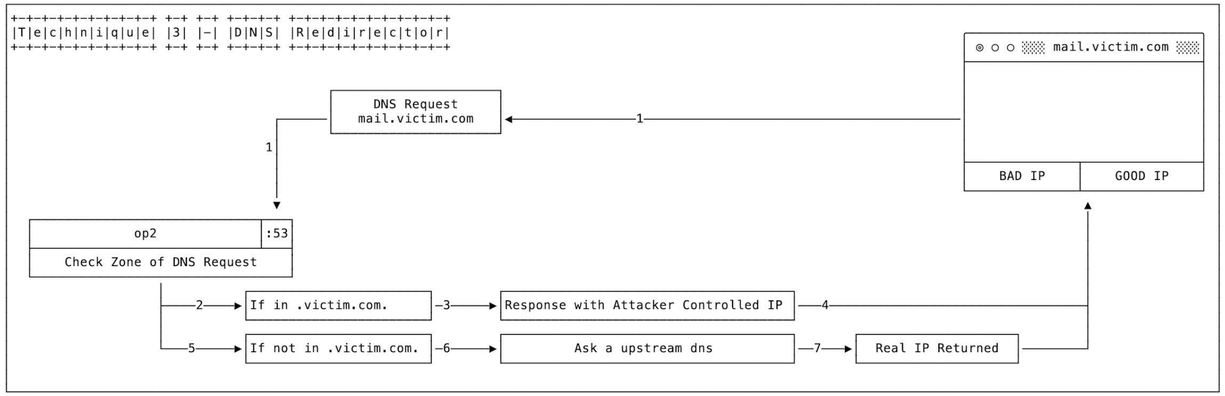
DNS Hijacking

A DNS hijacking is occurring at an unprecedented scale. Clever tricks allows attackers to obtain valid TLS certificate for hijacked domains.

https://arstechnica.com/information-technology/2019/01/a-dns-hijacking-wave-is-targeting-companies-at-an-almost-unprecedented-scale/







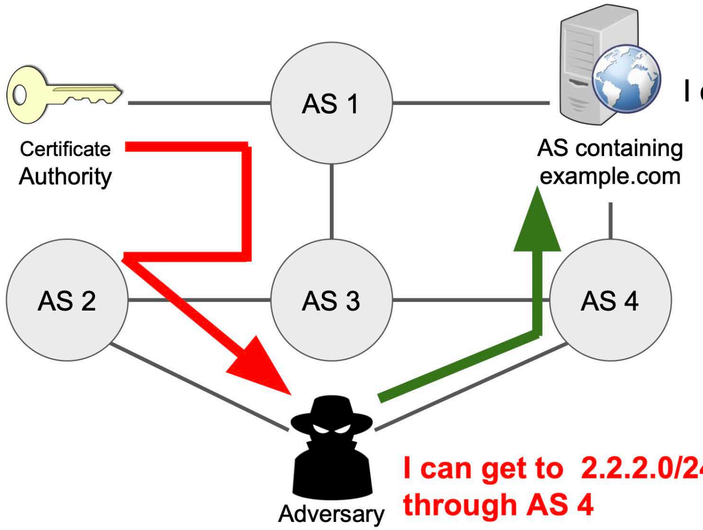
BGP Hijacking: AS Path Poisoning

Spoof domain verification process from CA. Allows attackers to obtain valid TLS certificate for hijacked domains.

Birge-Lee, H., Sun, Y., Edmundson, A., Rexford, J. and Mittal, P., "Bamboozling certificate authorities with {BGP}," vol. 27th {USENIX} Security Symposium, no. {USENIX} Security 18, pp. 833-849, 2018 https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee

Gavrichenkov, A., "Breaking HTTPS with BGP Hijacking," BlackHat, 2015 https://www.blackhat.com/docs/us-15/materials/us-15-Gavrichenkov-Breaking-HTTPS-With-BGP-Hijacking-wp.pdf

AS path poisoning

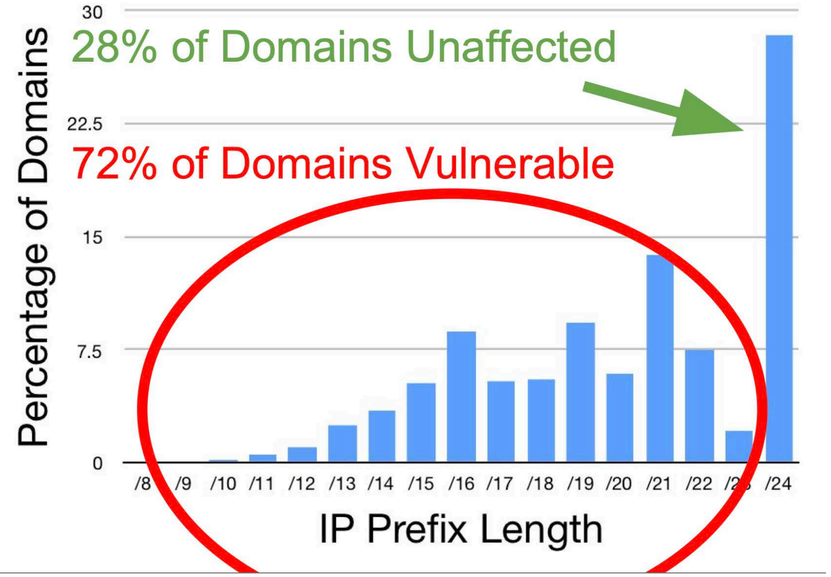


I own 2.2.2.0/23

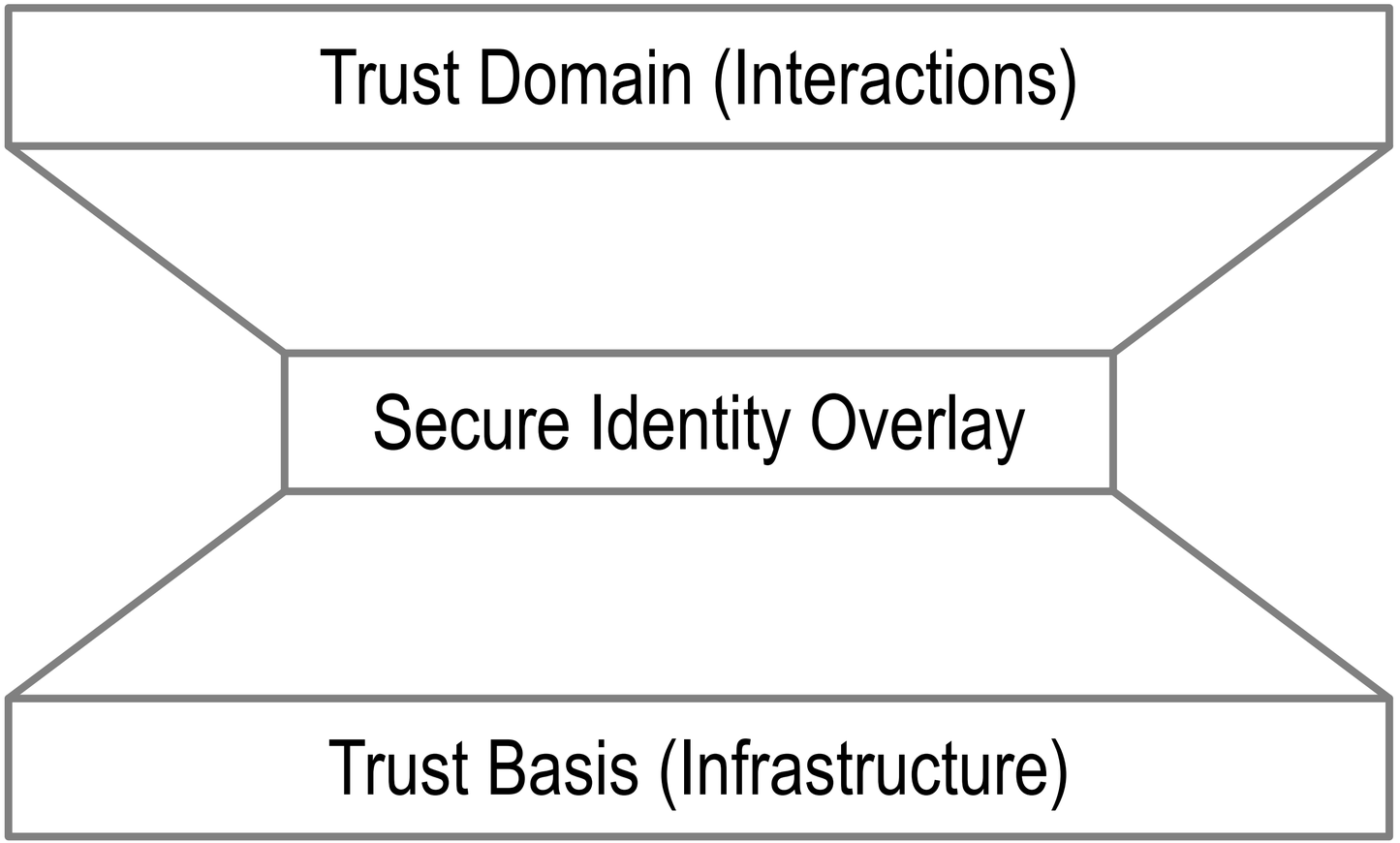
- Everyone sees announcement but looks less suspicious
- Connectivity preserved
- Almost any AS can perform
- Very stealthy
- Perfect setup to intercept traffic with certificate

Vulnerability of domains: sub-prefix attacks

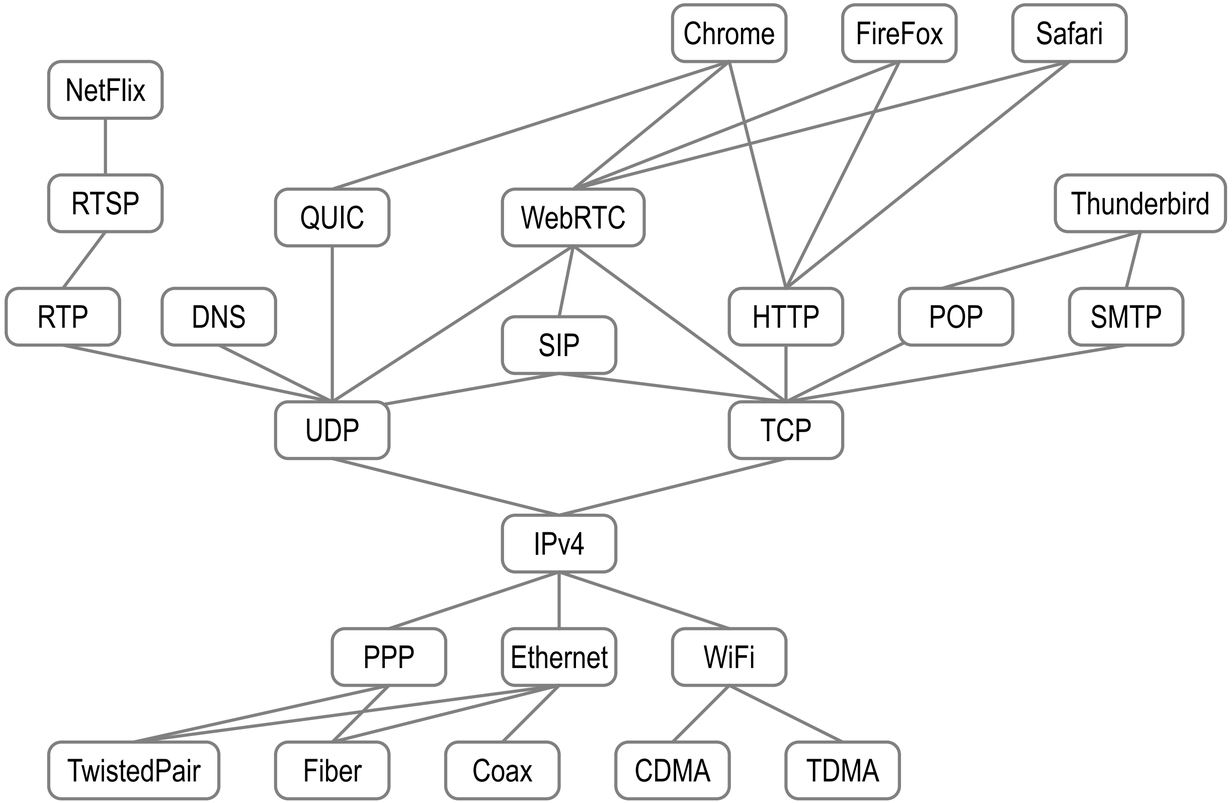
- Any AS can launch
- Only prefix lengths less than /24 vulnerable (filtering)

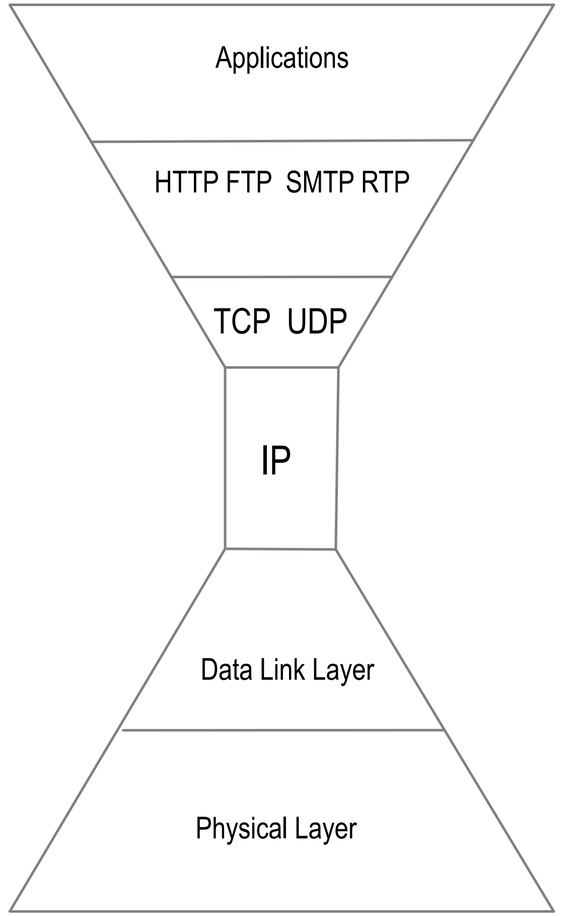


Identity System Security Overlay



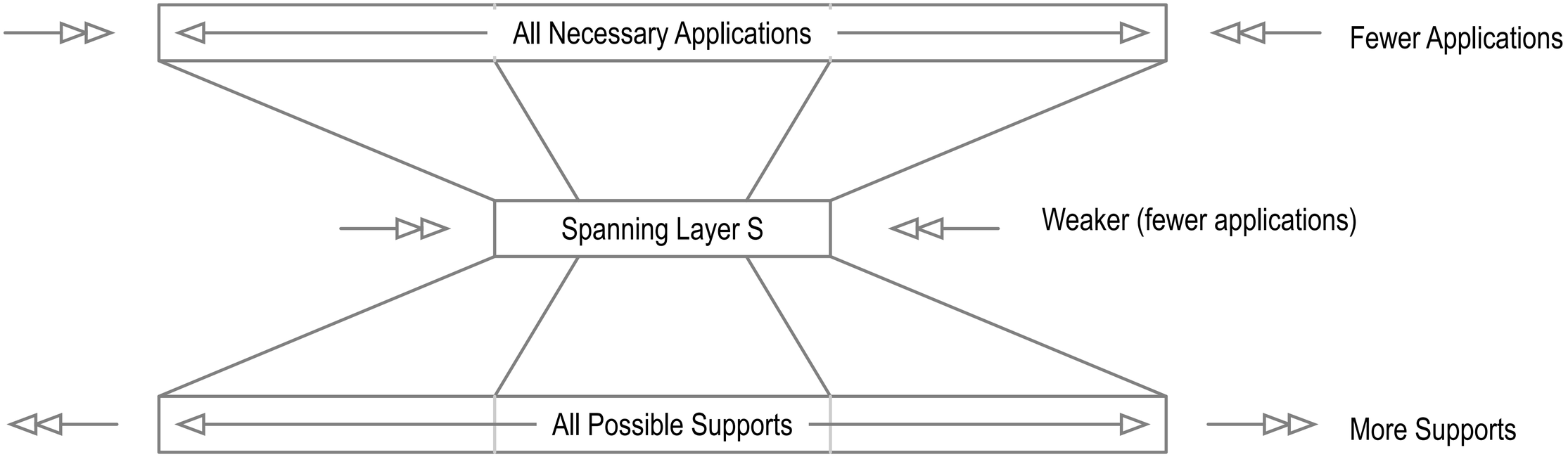
Spanning Layer





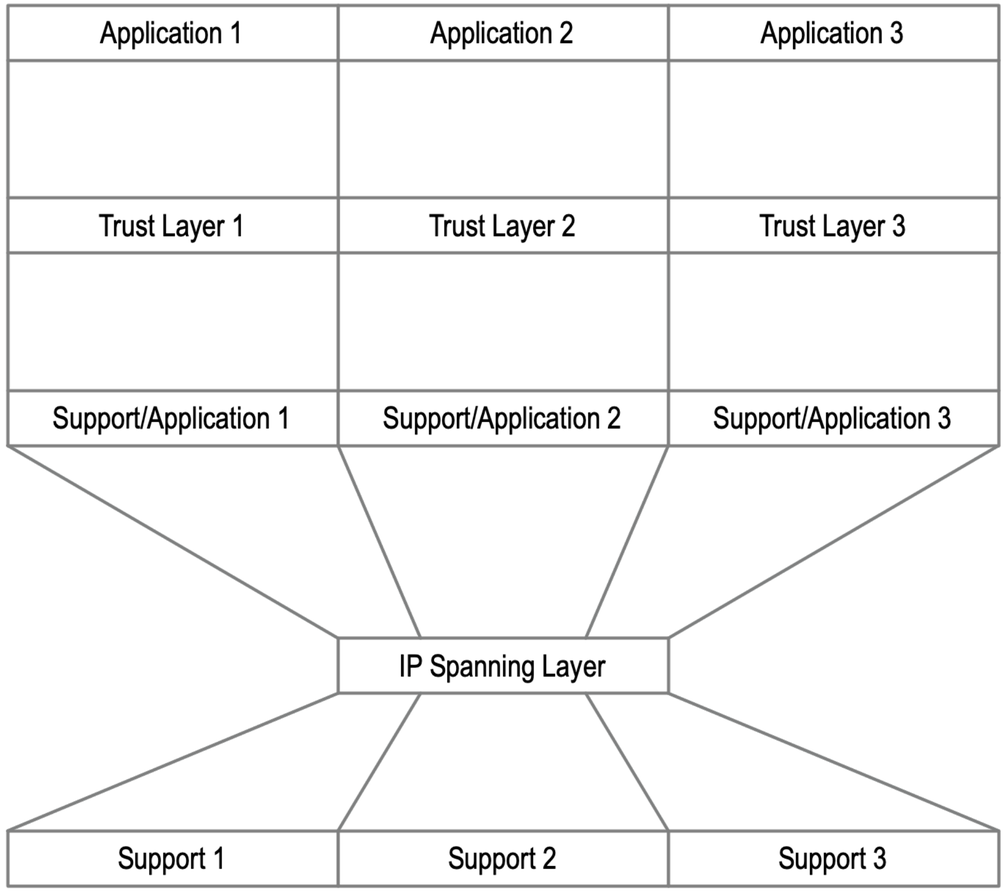
https://web.archive.org/web/20050415042854/http://www.csd.uch.gr/~hy490-05/lectures/Clark_interoperation.htm

Hourglass

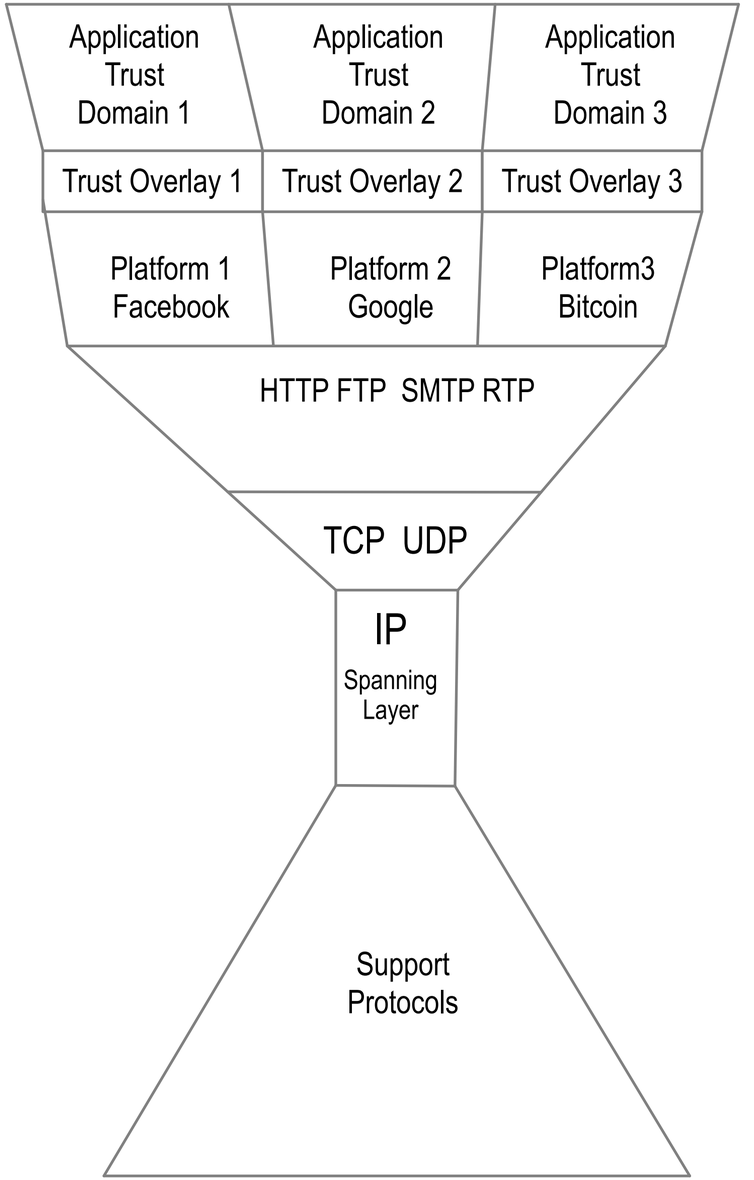


https://cacm.acm.org/magazines/2019/7/237714-on-the-hourglass-model/fulltext

Platform Locked Trust



Trust Domain Based Segmentation

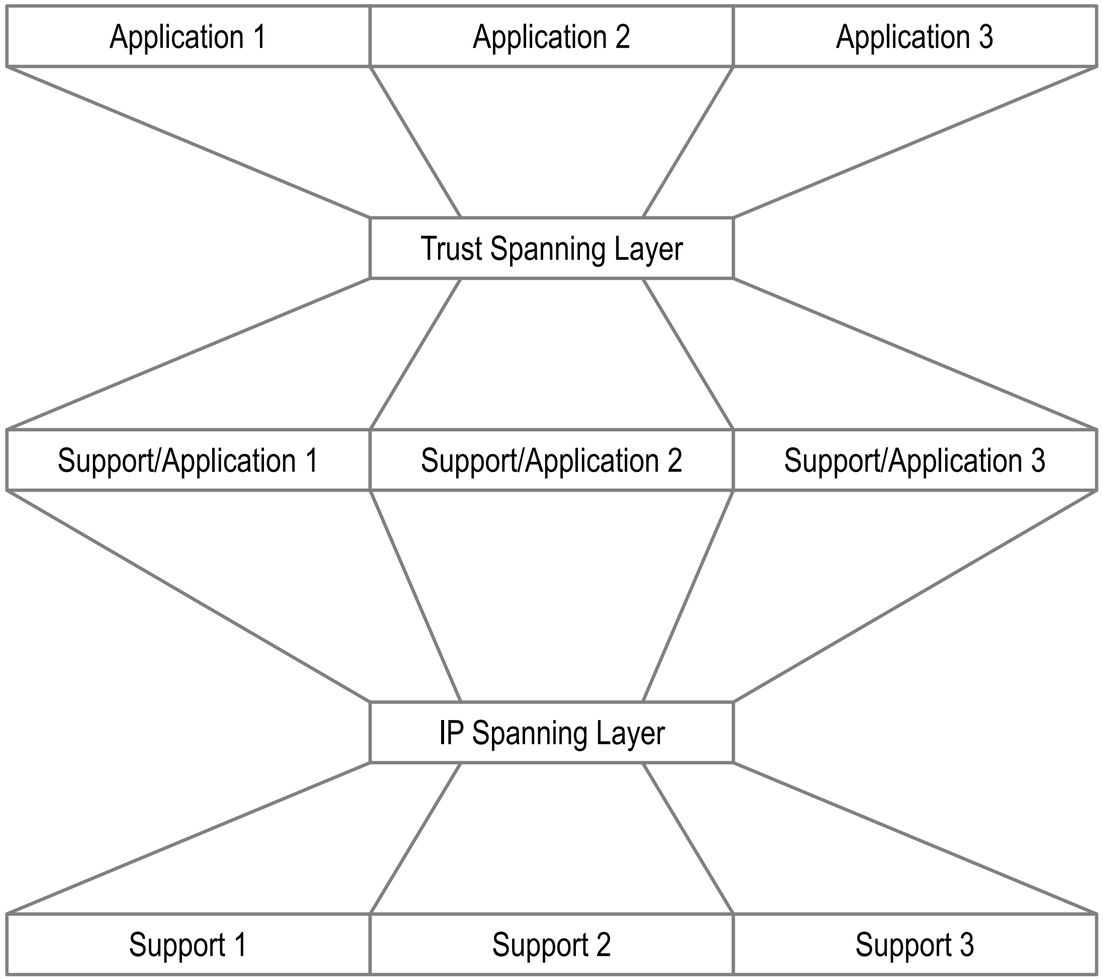


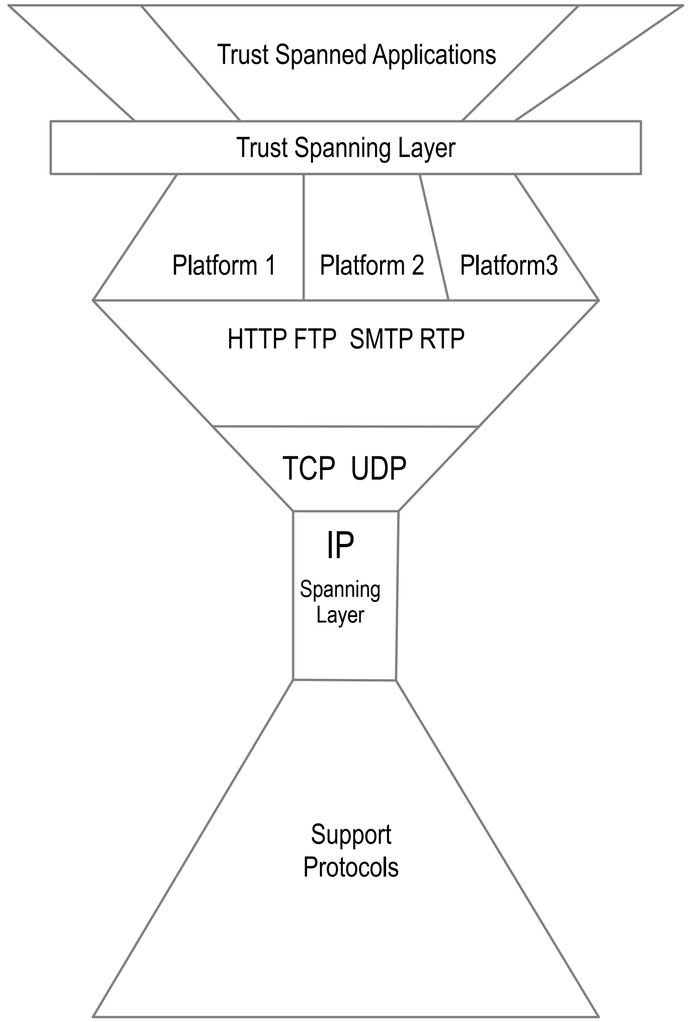
Each trust layer only spans platform specific applications

Bifurcated internet trust map

No *spanning* trust layer

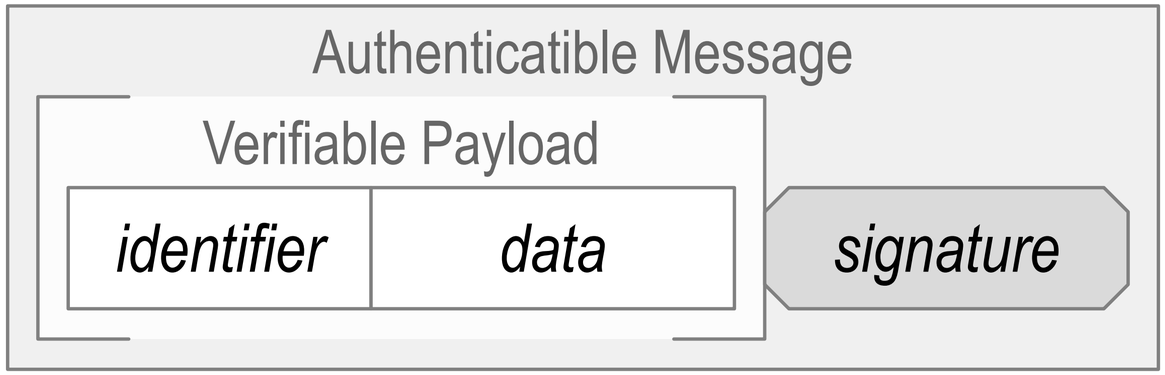
Solution: Waist and Neck



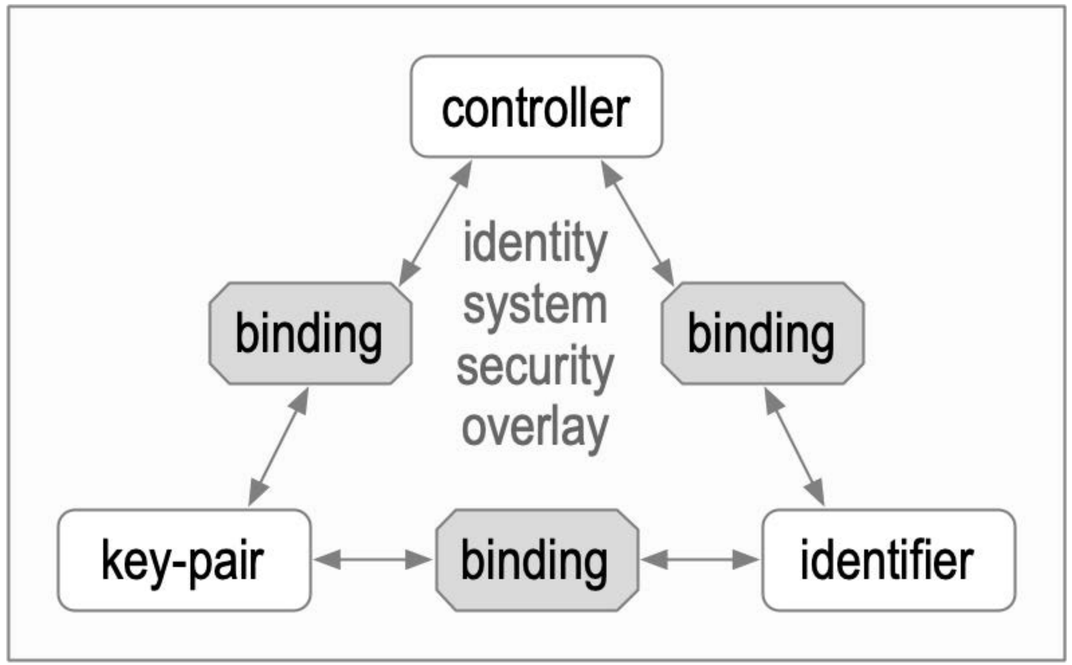


Identity System Security Overlay

Establish authenticity of IP packet's message payload.



The overlay's security is contingent on the mapping's security.



Identifier Issuance

KERI is not Identity Proofing?

KERI Identifiers are pseudonymous = high entropy pseudo random strings of characters

`EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148`

A given KERI Identifier may be associated with a natural person or legal entity via identity proofing

The advantage of KERI is that this association need only be made once at inception.

The association persists in spite of change of control of the identifier via rotation of its keys.

KERI provides persistent control of its pseudonymous identifiers in spite of key rotations.

KERI uses pre-rotation, a forward blinded commitment to a rotation key to replace signing keys.

Rotation keys are one-time only.

KERI provides recovery of control of an identifier in spite of signing key compromise.

What is KERI?

Key Event Receipt Infrastructure: Decentralized Key Management Infrastructure

KERI fixes the security flaw (authenticity) in PKI (Public Key Infrastructure).

The flaw in PKI is key rotation.

> Authorship is established in PKI with asymmetric (public, private) signing key pairs.

KERI solves the key rotation problem for control over an identifier

KERI uses portable verifiable data structures called *key event logs* (KELs) to provide duplicity evident proof of the controlling key state for pseudonymous cryptographic self-certifying identifiers (SCIDs).

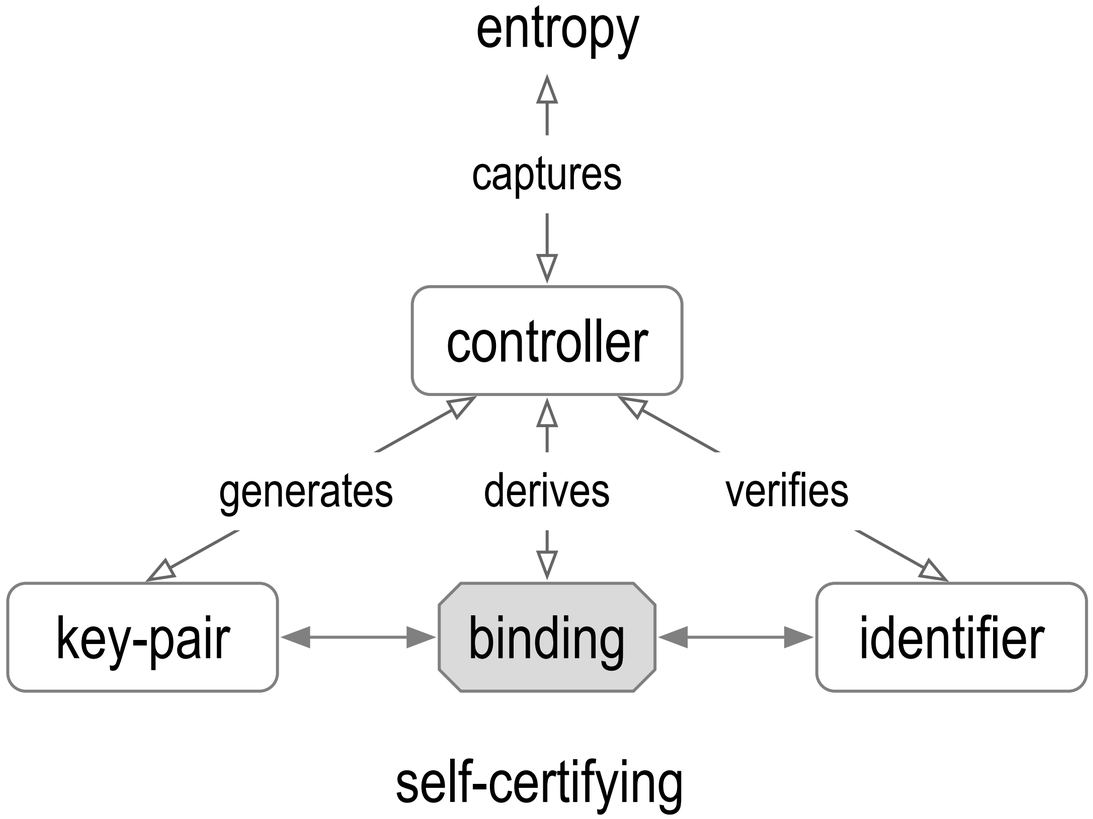
With KERI, key state is cryptographically verifiably bound to self-certifying identifiers

In contrast conventional PKI uses assertions made by trusted entities to bind key state to identifiers

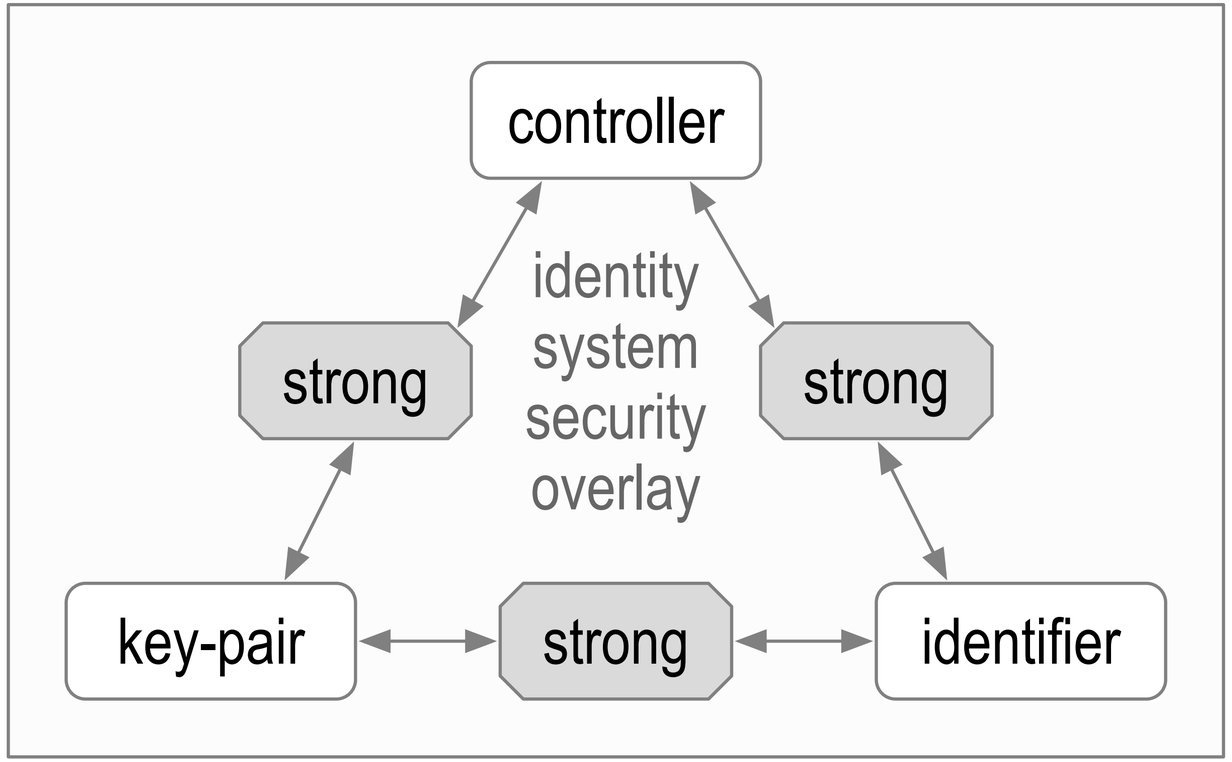
KERI solves the *secure attribution* problem with zero trust.

> Every statement associated with an identifier may be non-repudiably and securely attributed to the controller of the identifier via a signature made with the keys determined by cryptographically verifiable key state.

Self-Certifying Identifier Issuance and Binding

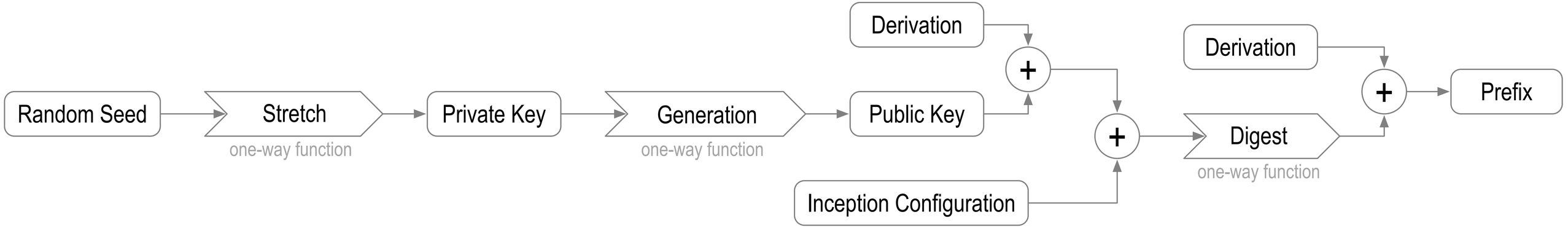


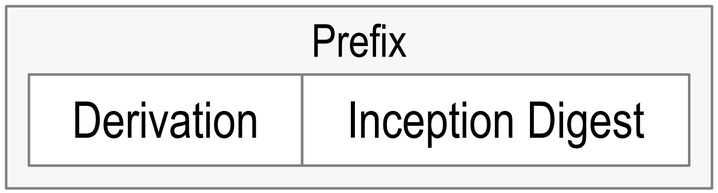
self-certifying

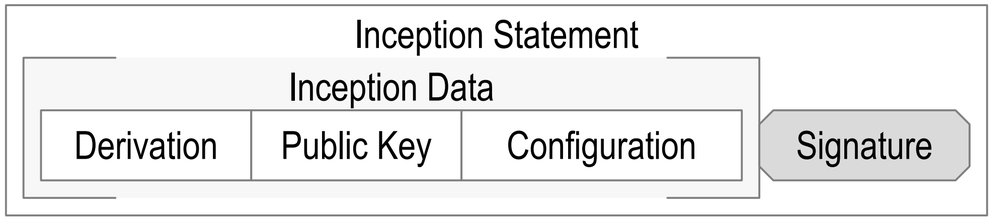


Self-Certifying Identifier Issuance

Self-Addressing SCID



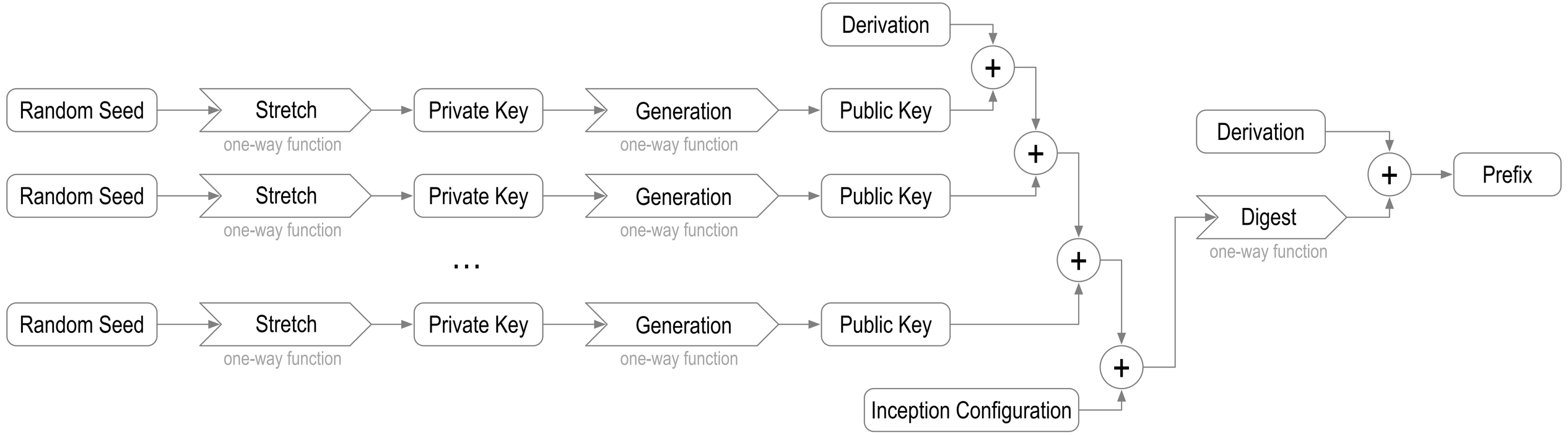


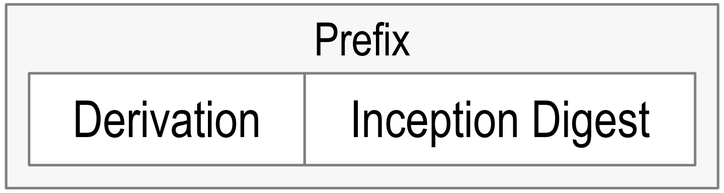


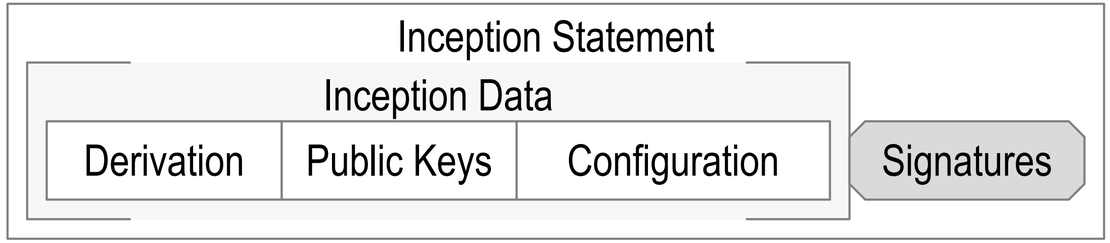
`EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148`

`did:keri:EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148/path/to/resource?name=secure#this`

Multi-Sig Self-Addressing SCID



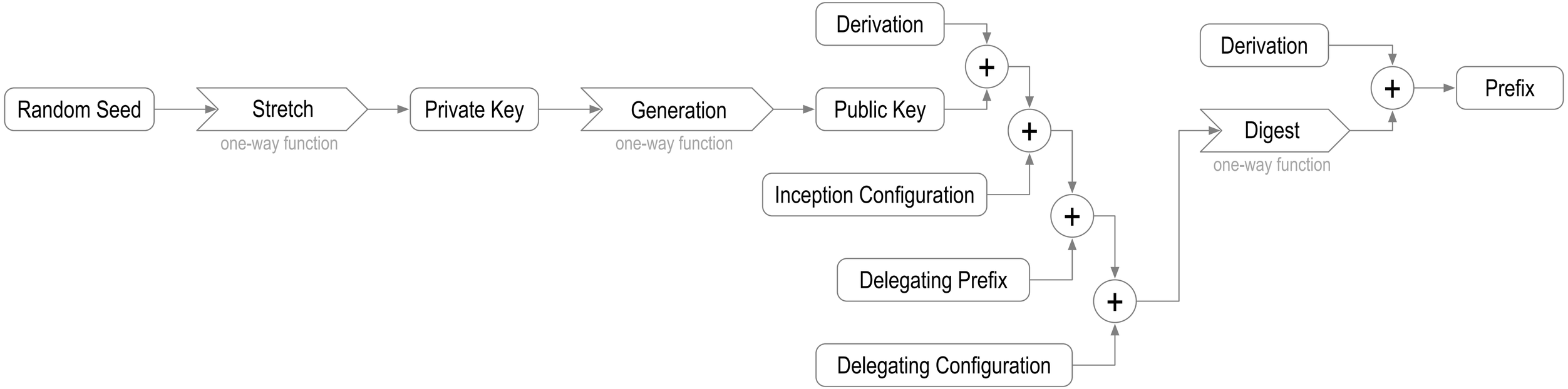


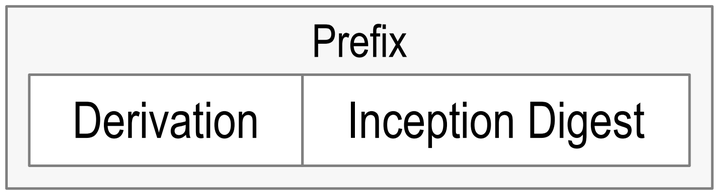


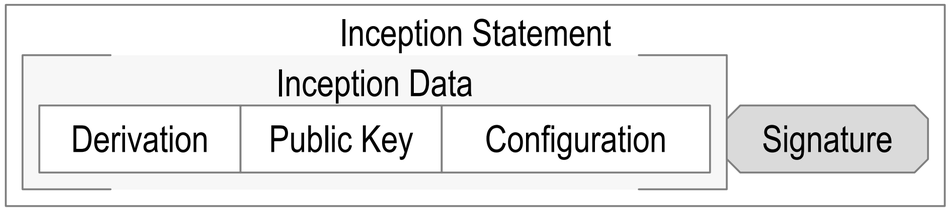
EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148

did:un:EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148/path/to/resource?name=secure#really

Delegated Self-Addressing SCID



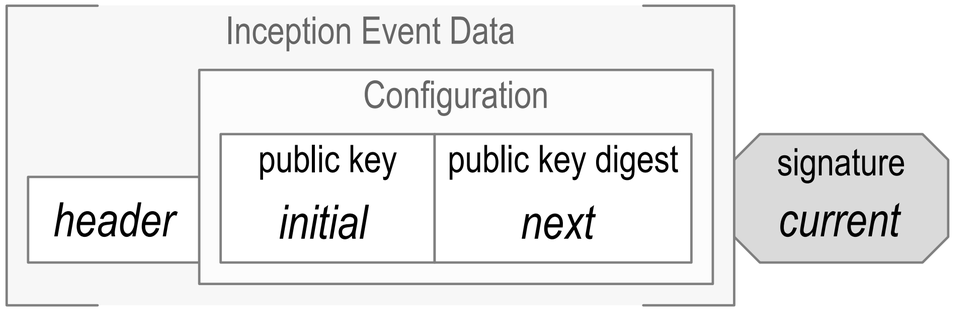


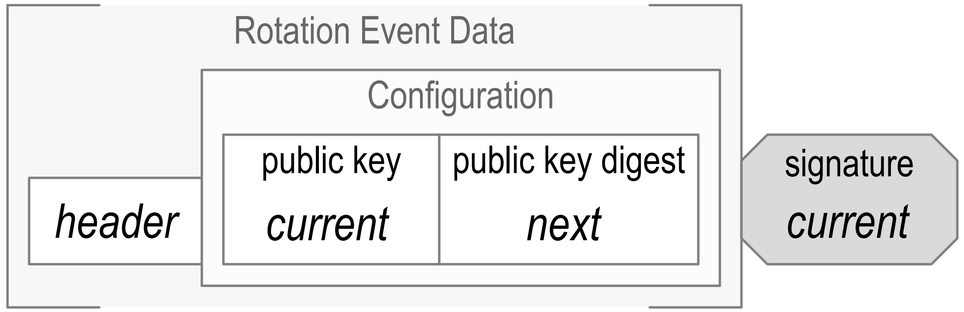


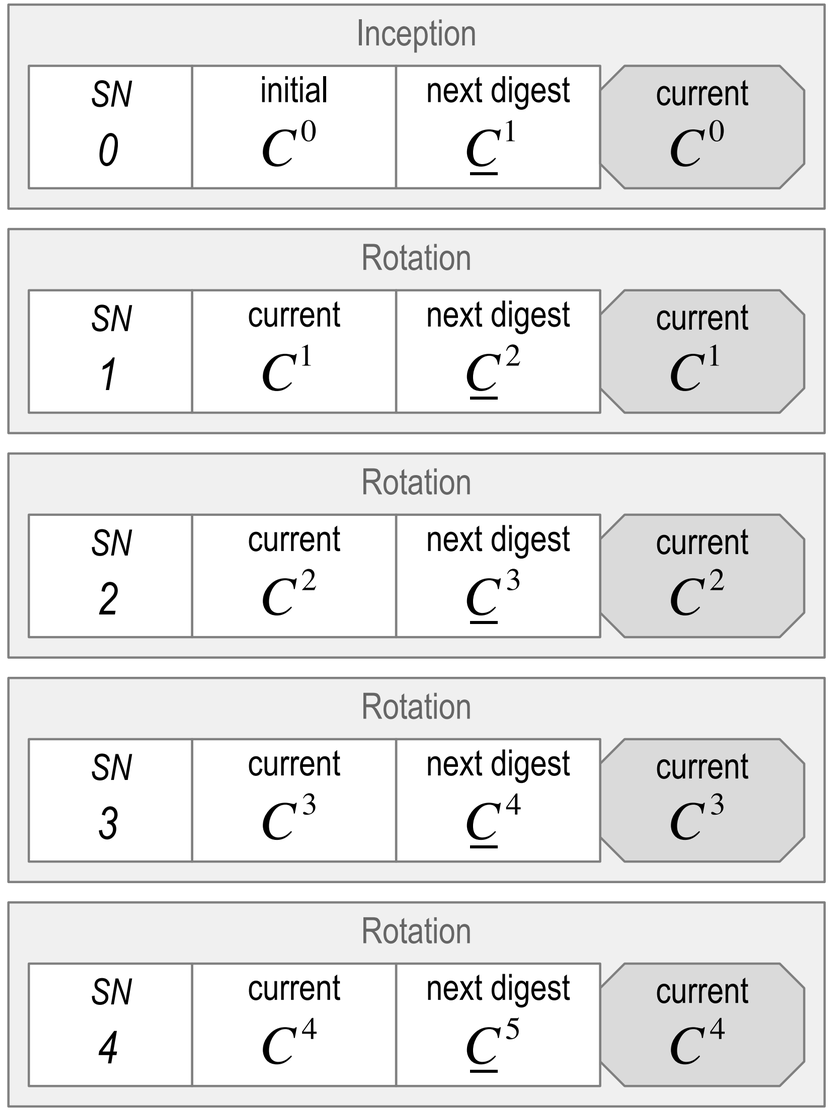
EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148

did:un:EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148/path/to/resource?name=secure#really

Pre-Rotation

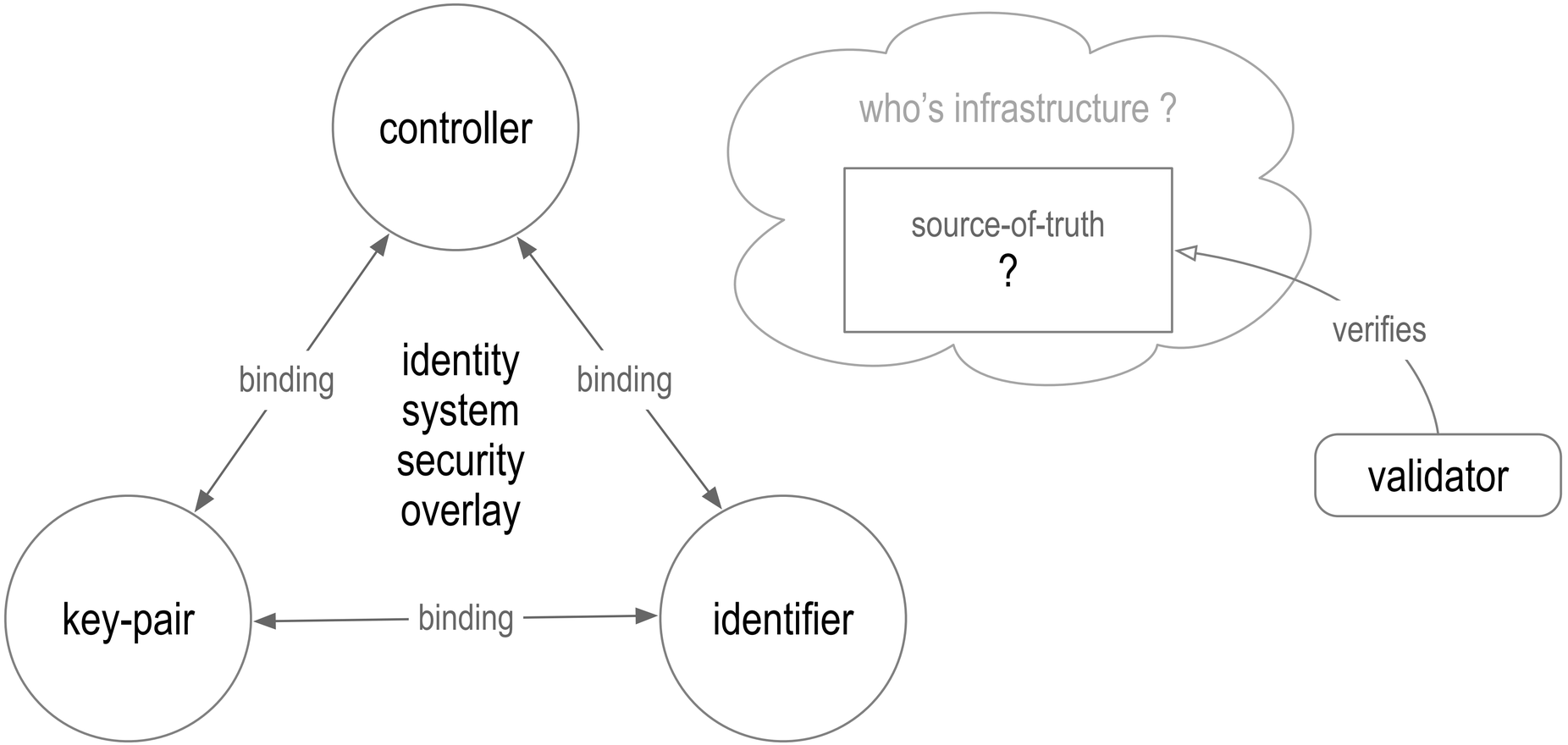






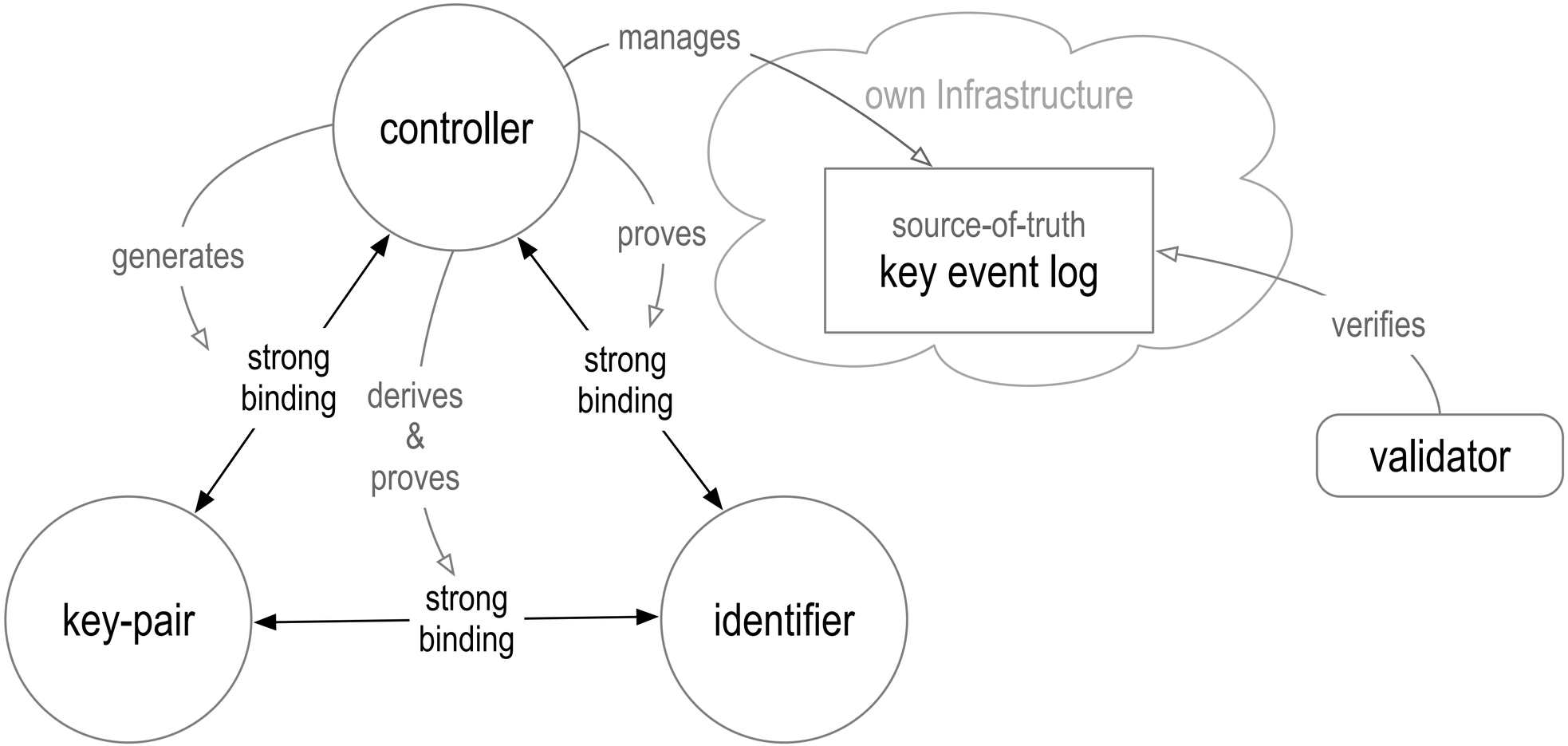
Digest of *next* key(s) makes pre-rotation post-quantum secure

Trust Basis


controller
who's infrastructure ?
source-of-truth
?
verifies
validator
binding
identity
system
security
overlay
binding
key-pair
binding
identifier

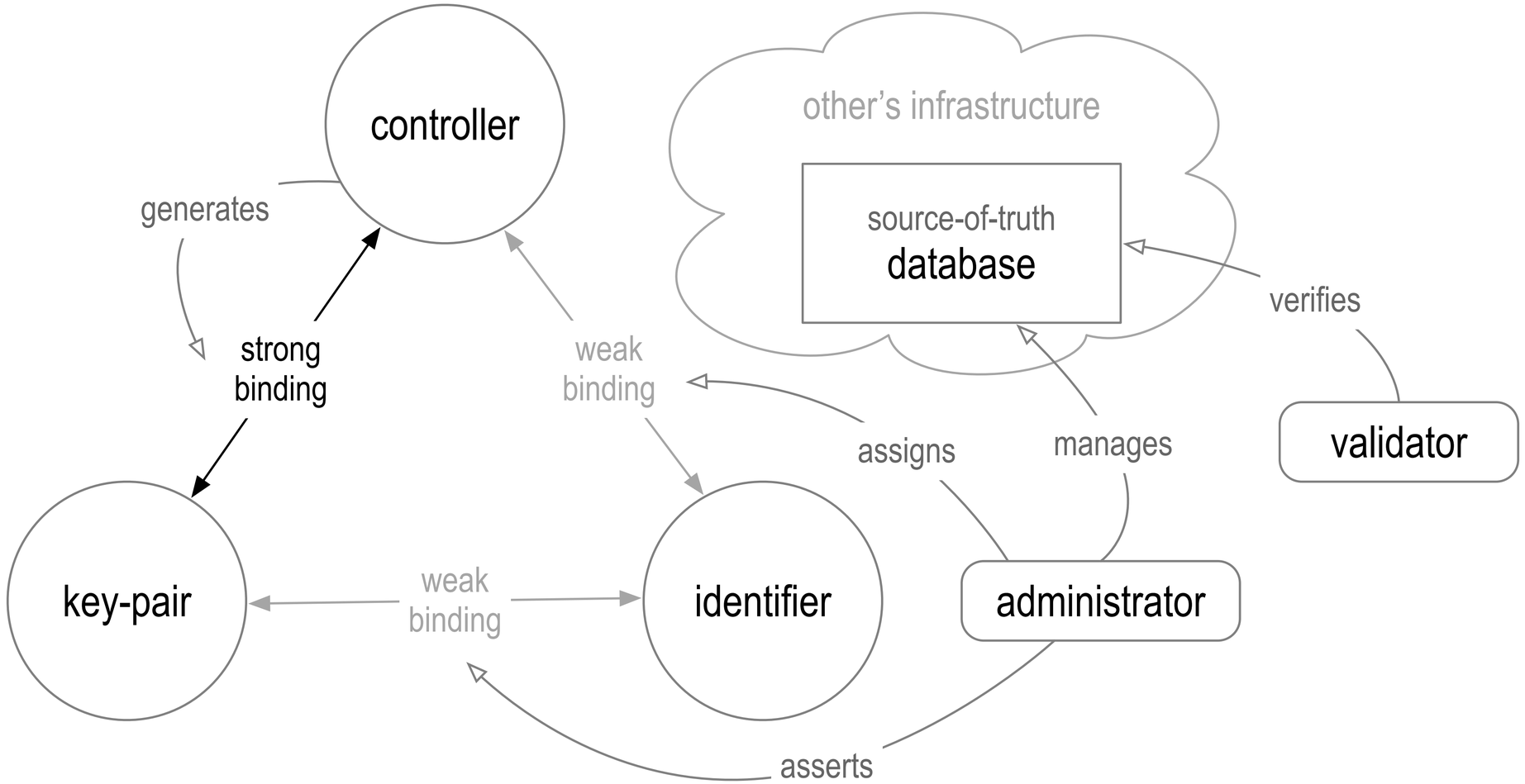
Autonomic Trust Basis

Cryptographic Proofs



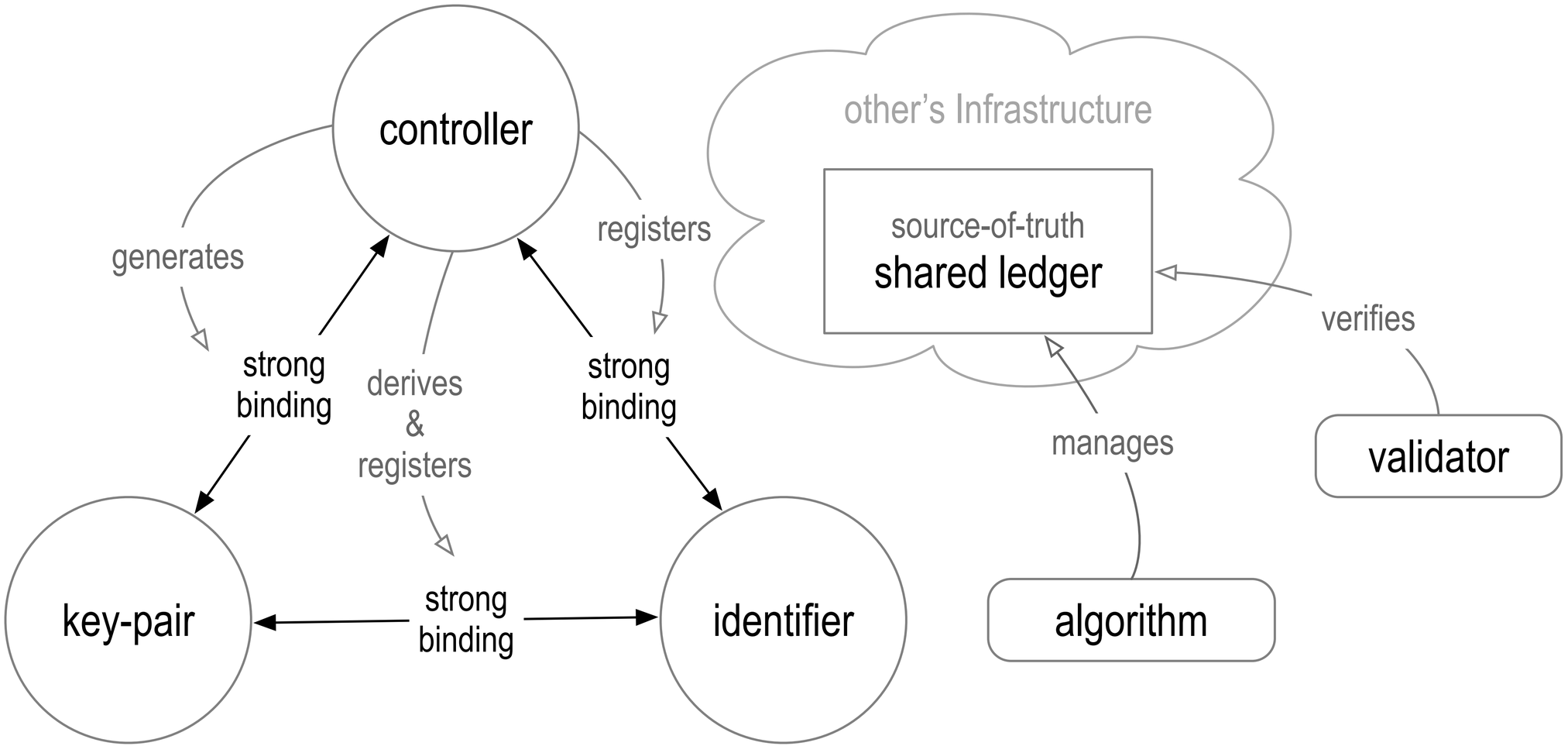
Administrative Trust Basis

DNS/Certificate Authorities

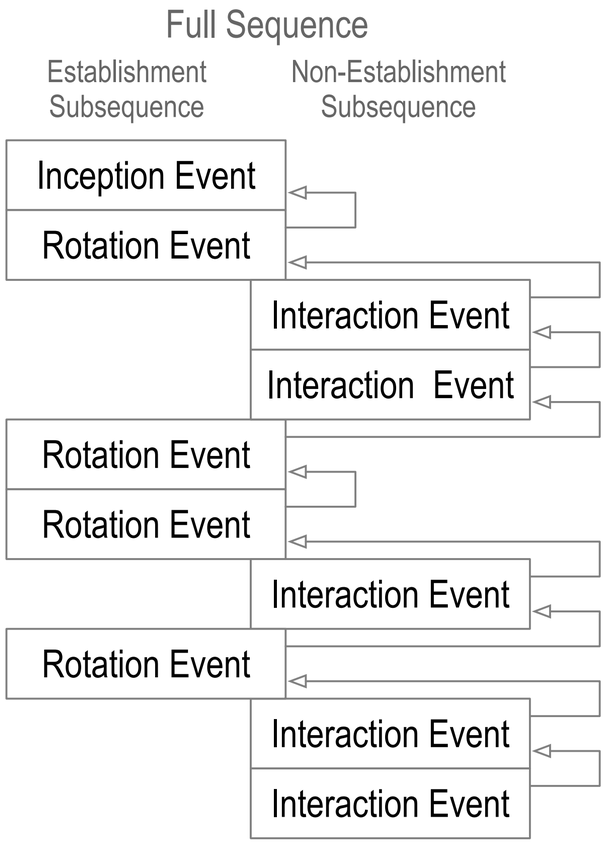


Algorithmic Trust Basis

Shared Distributed Ledgers



Inconsistency and Duplicity



inconsistency: lacking agreement, as two or more things in relation to each other

duplicity: acting in two different ways to different people concerning the same matter

Internal vs. External Inconsistency

Internally inconsistent log = not verifiable.

Log verification from self-certifying root-of-trust protects against internal inconsistency.

Externally inconsistent log with a purported copy of log but both verifiable = duplicitous.

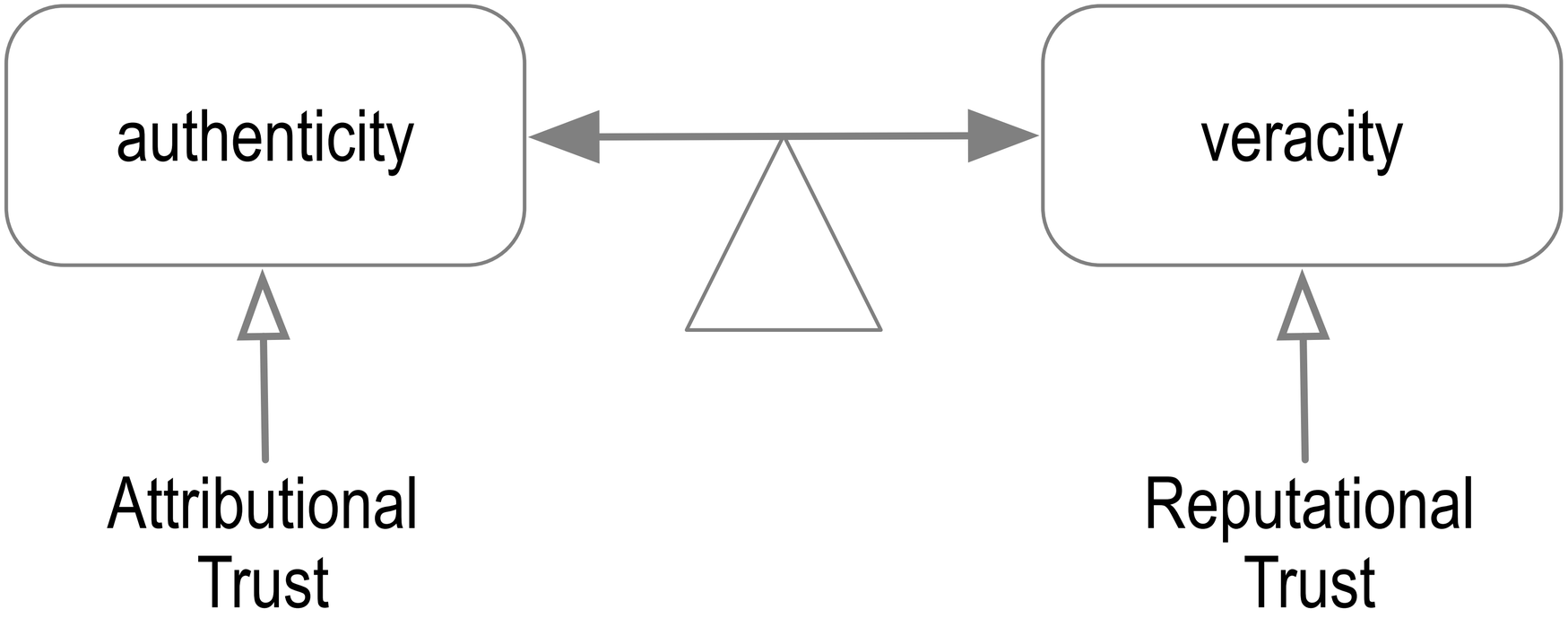
Duplicity detection protects against external inconsistency.

KERI provides duplicity evident DKMI

To Learn More About KERI.

https://keri.one

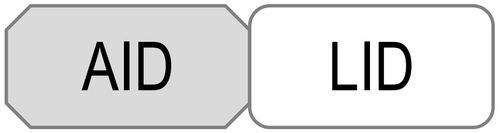
Trust Balance



Cryptographic

Behavioral

Unified Identifier Model



AID: Autonomic Identifier (primary)

self-managing self-certifying identifier with cryptographic root of trust

secure, decentralized, portable, universally unique

L*ID*: Legitimized Human Meaningful Identifier (secondary)

legitimized within trust domain of given AID by a verifiable authorization from AID controller

authorization is verifiable to the root-of-trust of AID

Forms *AID*|*LID* couplet within trust domain of AID

AID|LID Couplet

625.127C125r

EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148|625.127C125r

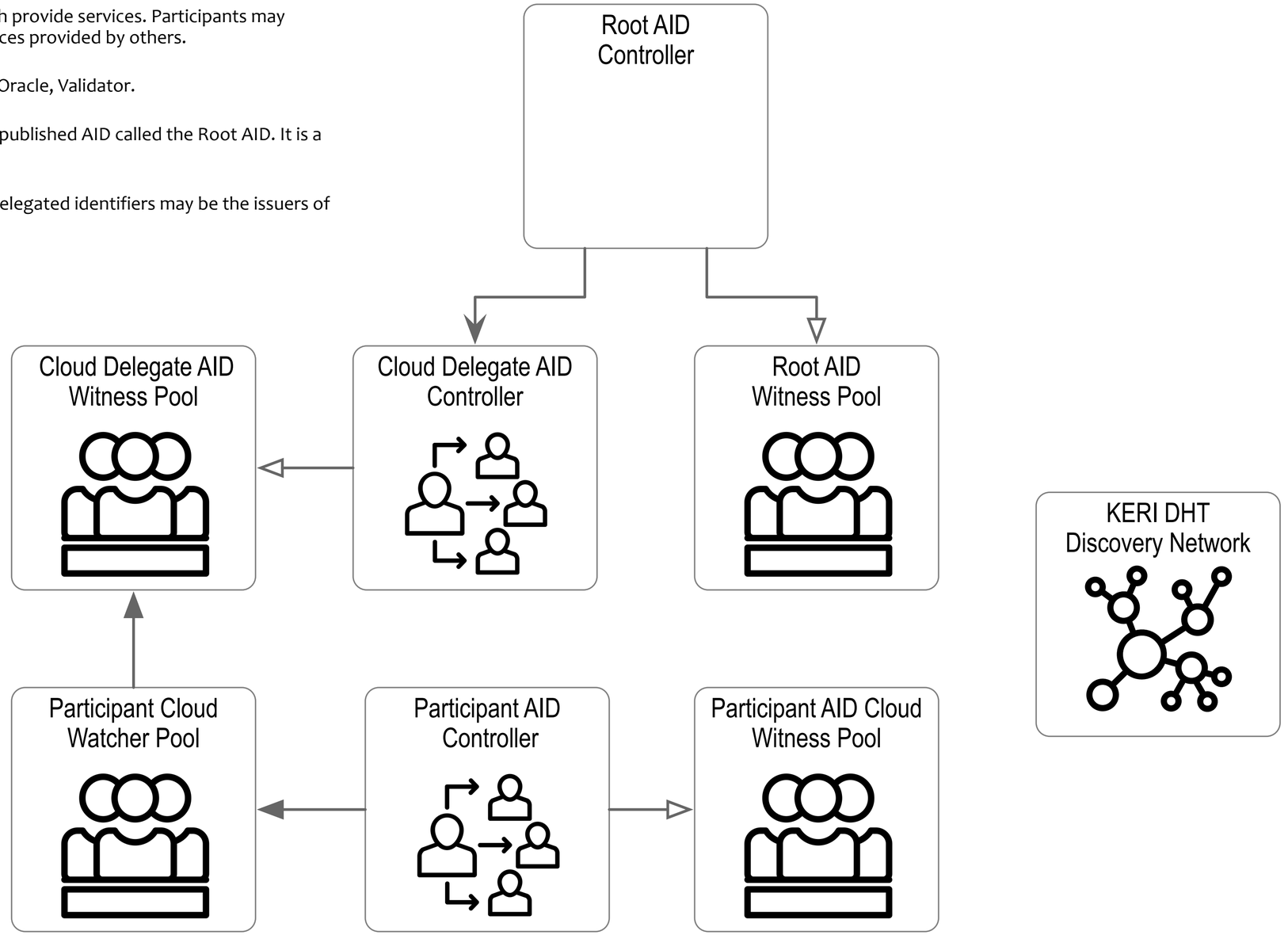
Basic KERI Stack

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.

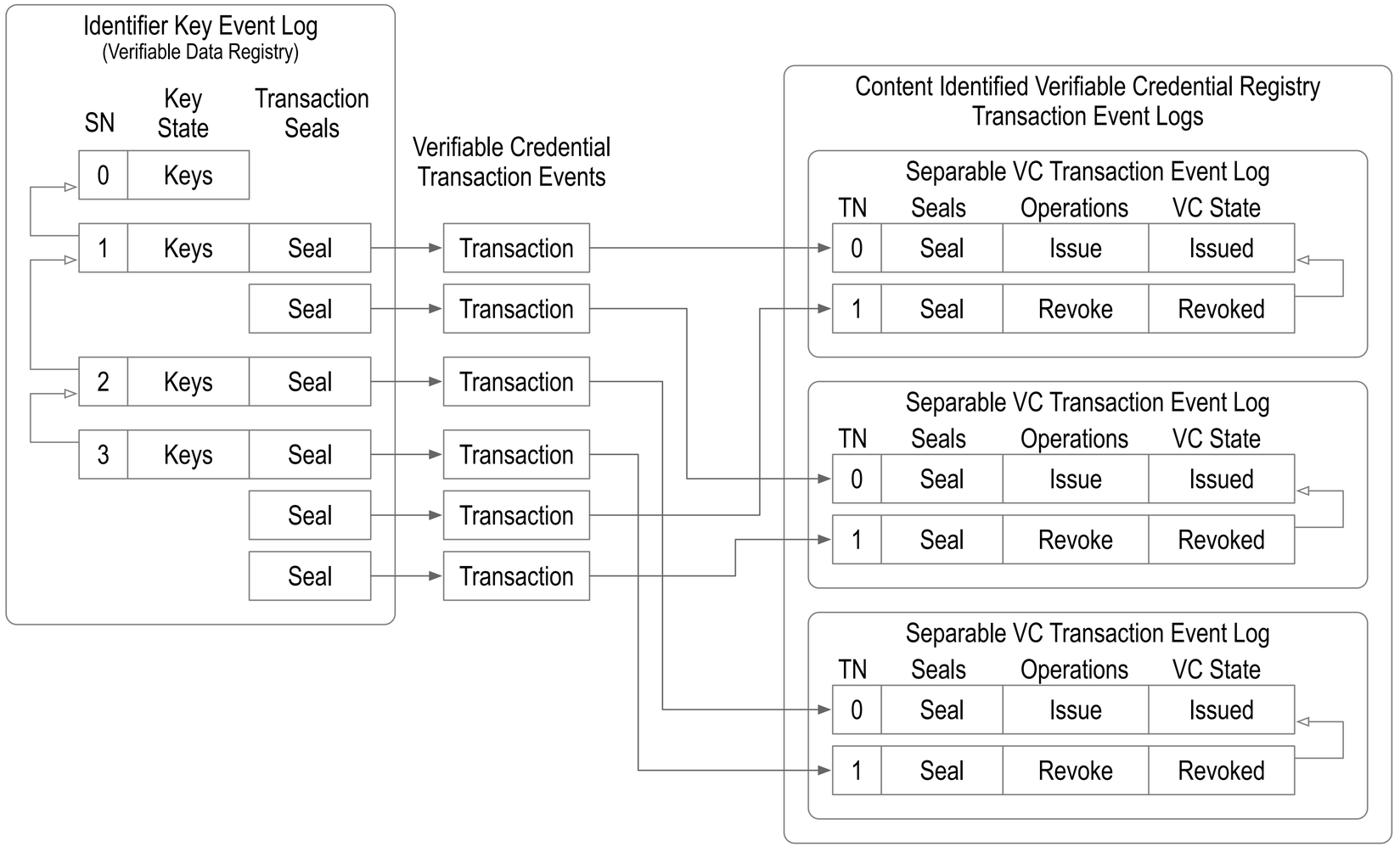
The component services include Controller, Witness, Watcher, Delegate, Oracle, Validator.

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

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



KEL Anchored Issuance-Revocation Registry with Separable VC TELs



Each VC has a uniquely self-addressing identifier (SAID)
Each VC has a uniquely identified issuer (AID)
Each VC may have a uniquely identified issuee (AID).
All VC Schema are immutable

Qualification testing of the vLEI Beta software

Participating in the sandbox

- Organizations confirmed for the review
  - 8 LEI Issuers
  - 4 external organizations

  (additional participation is expected)

- Functionality covered
  - vLEI Credential issuance scenarios (creating vLEIs)
  - vLEI Credential presentation scenarios (using vLEIs)
  - Identifier and Key Management scenarios

    (ensuring a secure vLEI infrastructure)
  - vLEI Credential revocation scenarios (‘retiring’ vLEIs)

- GLEIF looks forward to the feedback received for GLEIF to consider for incorporation into the version to be used for the vLEI pilots
  - Feedback encouraged until mid-November
  - Sandbox will be in place until year-end 2021