Duplicity Evident Data

How to protect verifiers (and controllers) from imposters without blockchain and trusted third parties

https://keri.one
https://github.com/WebOfTrust

Samuel M. Smith Ph.D.
sam@keri.one

Resources

Documentation:
https://keri.one/keri-resources/

KERI/ACDC Community: (meetings, open source code Apache2, specification drafts)
https://github.com/WebOfTrust
https://github.com/WebOfTrust/keri

ToIP: (meetings, specifications OWF License)
https://trustoverip.org/
https://wiki.trustoverip.org/display/HOME/ACDC+(Authentic+Chained+Data+Container)+Task+Force
https://wiki.trustoverip.org/display/HOME/Trust+Spanning+Protocol+Task+Force

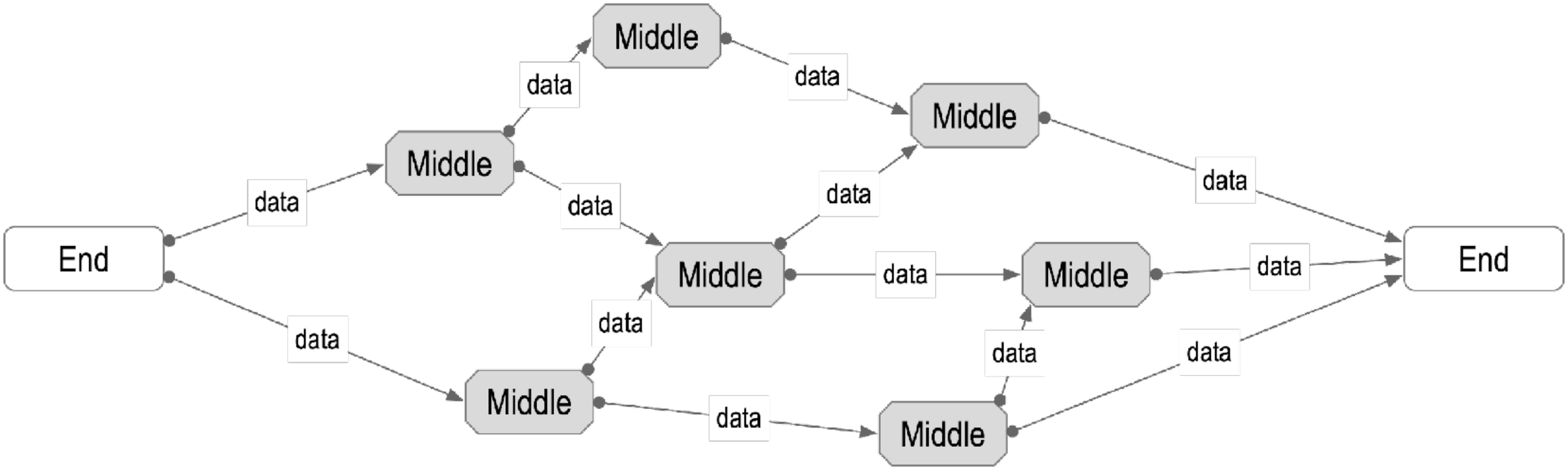
GLEIF:
https://www.gleif.org/en/lei-solutions/gleifs-digital-strategy-for-the-lei/introducing-the-verifiable-lei-vlei

healthKERI:
https://healthkeri.com/

KERI GLEIF TRUST Over IP FOUNDATION ISO DirectTrust® healthKERI

End Verifiability

End-to-End Verifiability



If the edges are secure, the security of the middle doesn't matter.

Ambient Verifiability: any-data, any-where, any-time by any-body

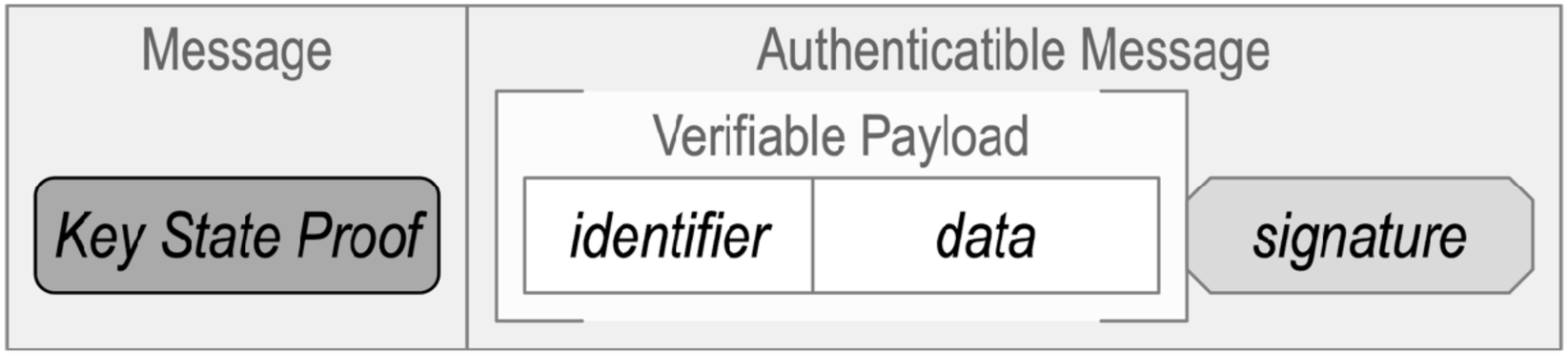
Zero-Trust-Computing

It's much easier to protect one's private keys than to protect everyone else's internet infrastructure

Identity (-ifier) System Security Overlay

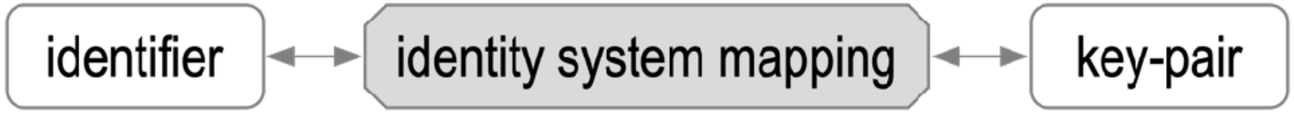
persistent mapping via verifiable data structure of key state changes

Establish authenticity of IP packet's message payload.

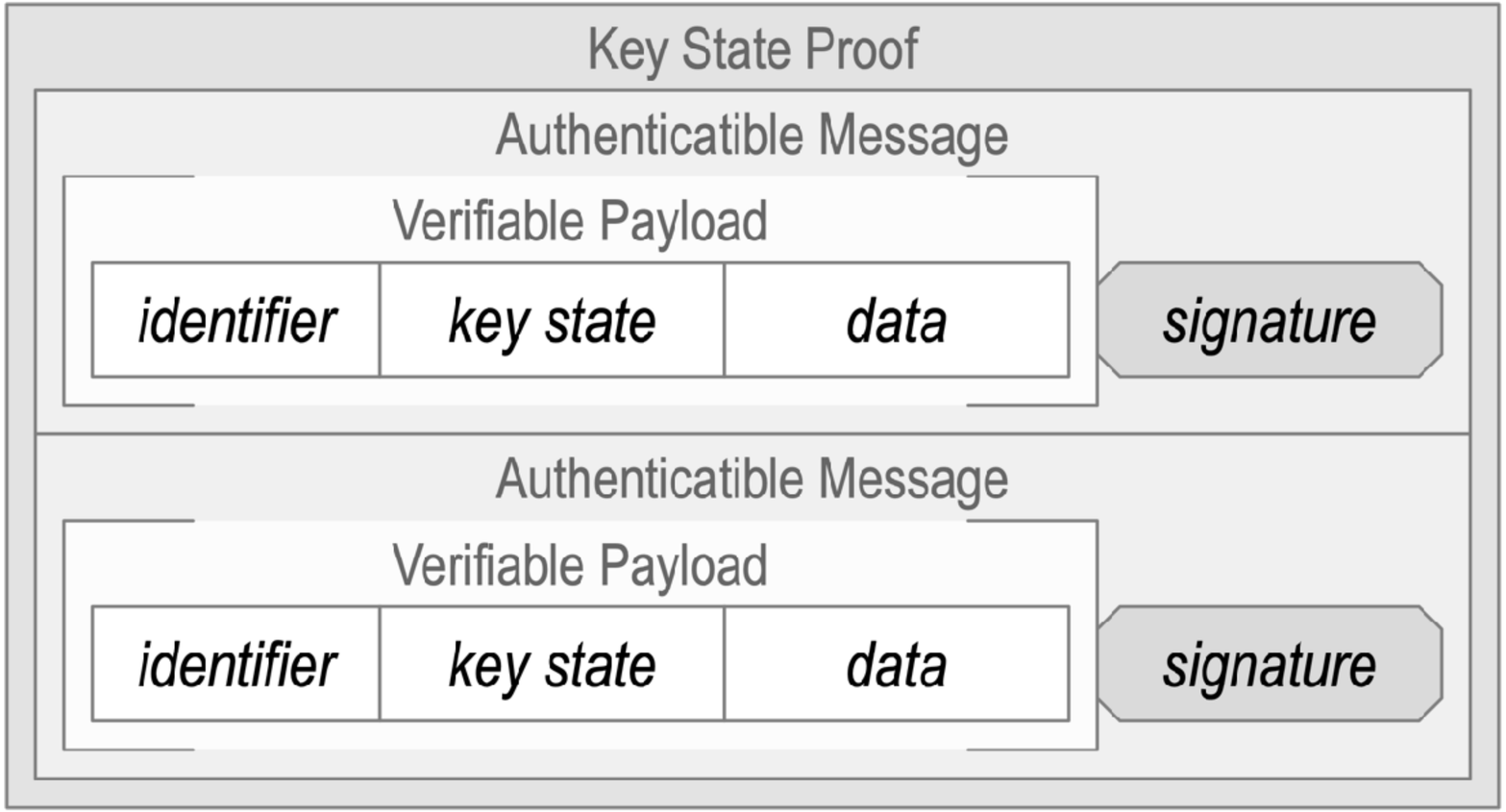


The overlay's security is contingent on the mapping's security.

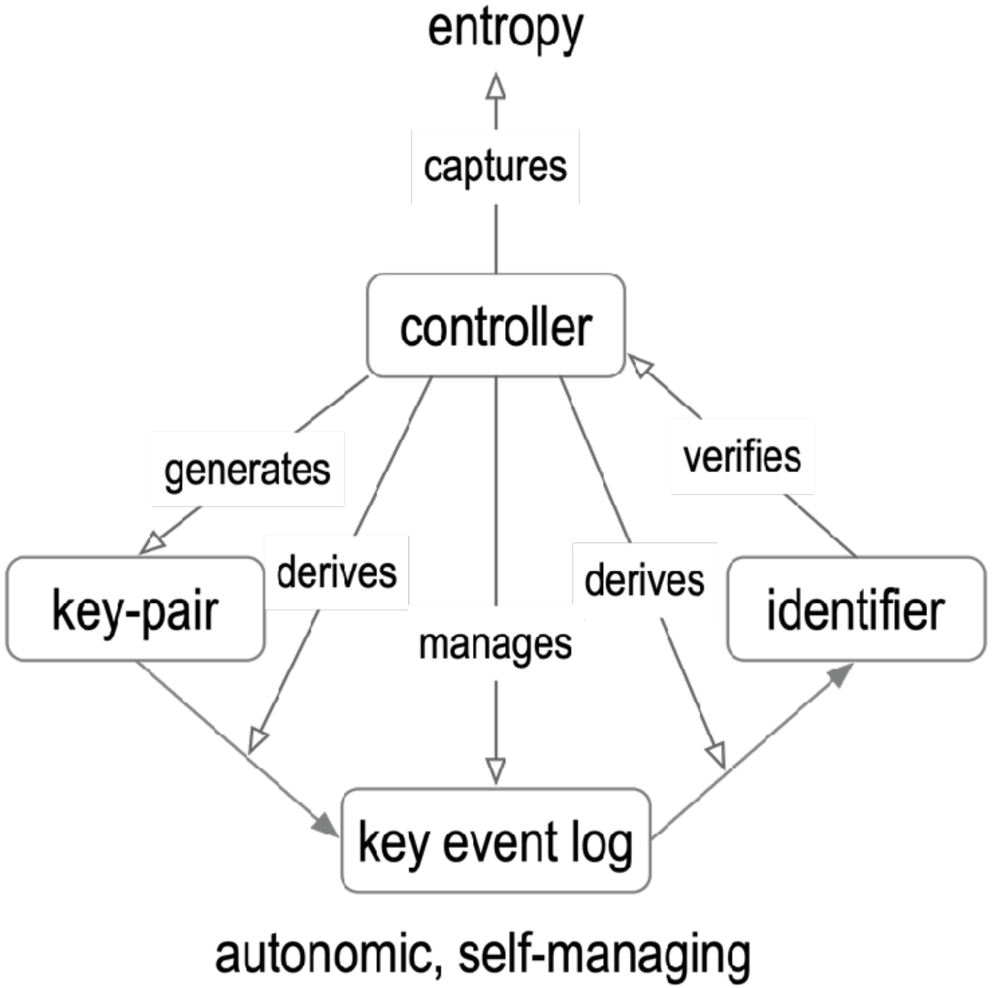
Key State Proof is Recursive Application of Overlay



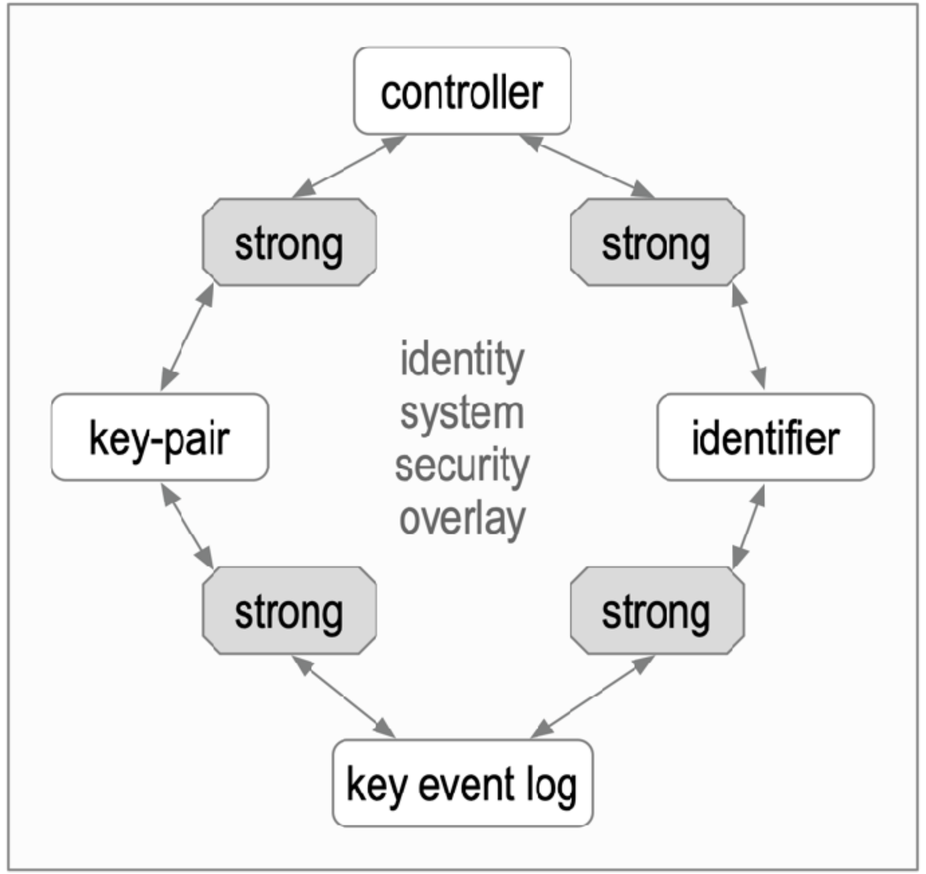
Persistent mapping via verifiable data structure of key state changes



Autonomic Identifiers (AIDs): (type of self-certifying identifier) Issuance and Binding



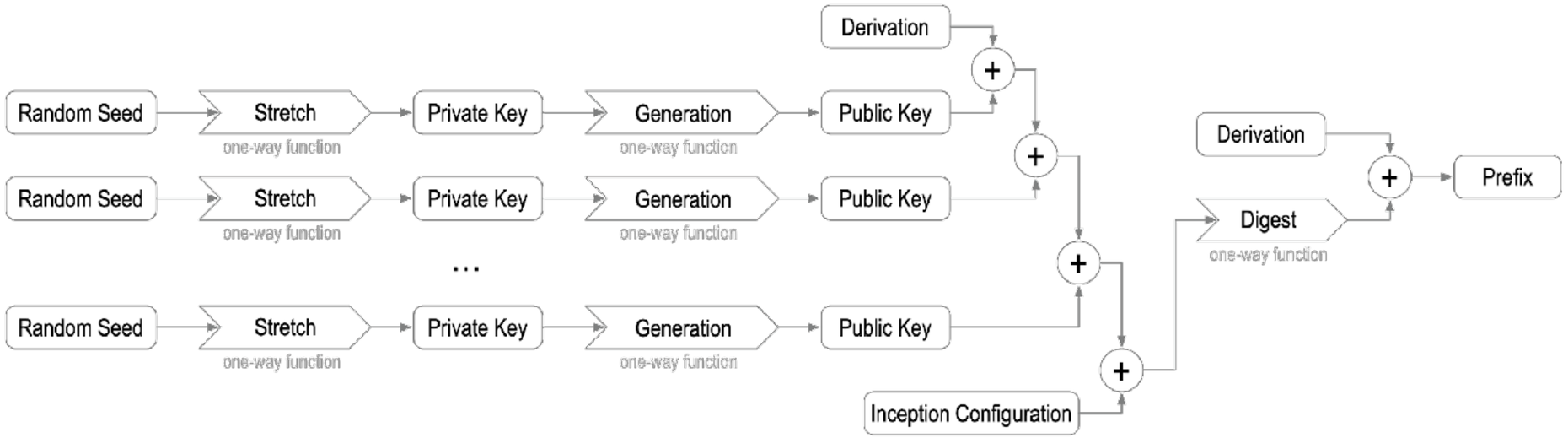
autonomic, self-managing

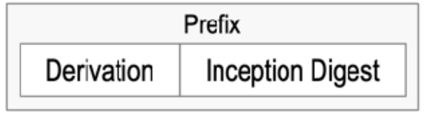


Autonomic Identifier Issuance Tetrad

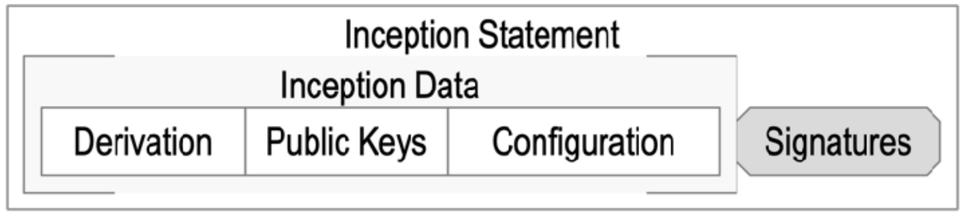
cryptographic root-of-trust with verifiable persistent control

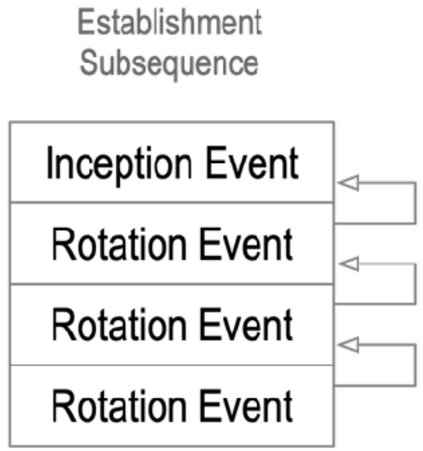
Cryptographic Root-of-Trust:
Self-Certifying Identifier (SCID) + Key Event Log = Autonomic Identifier (AID)





Key Event Log



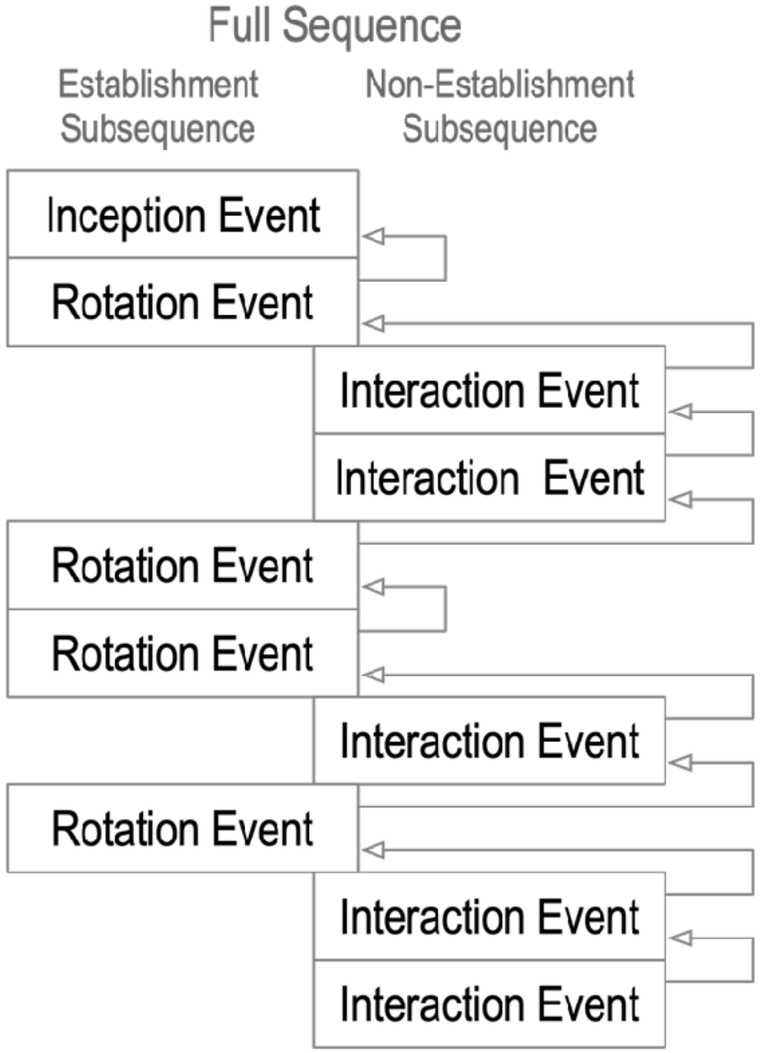


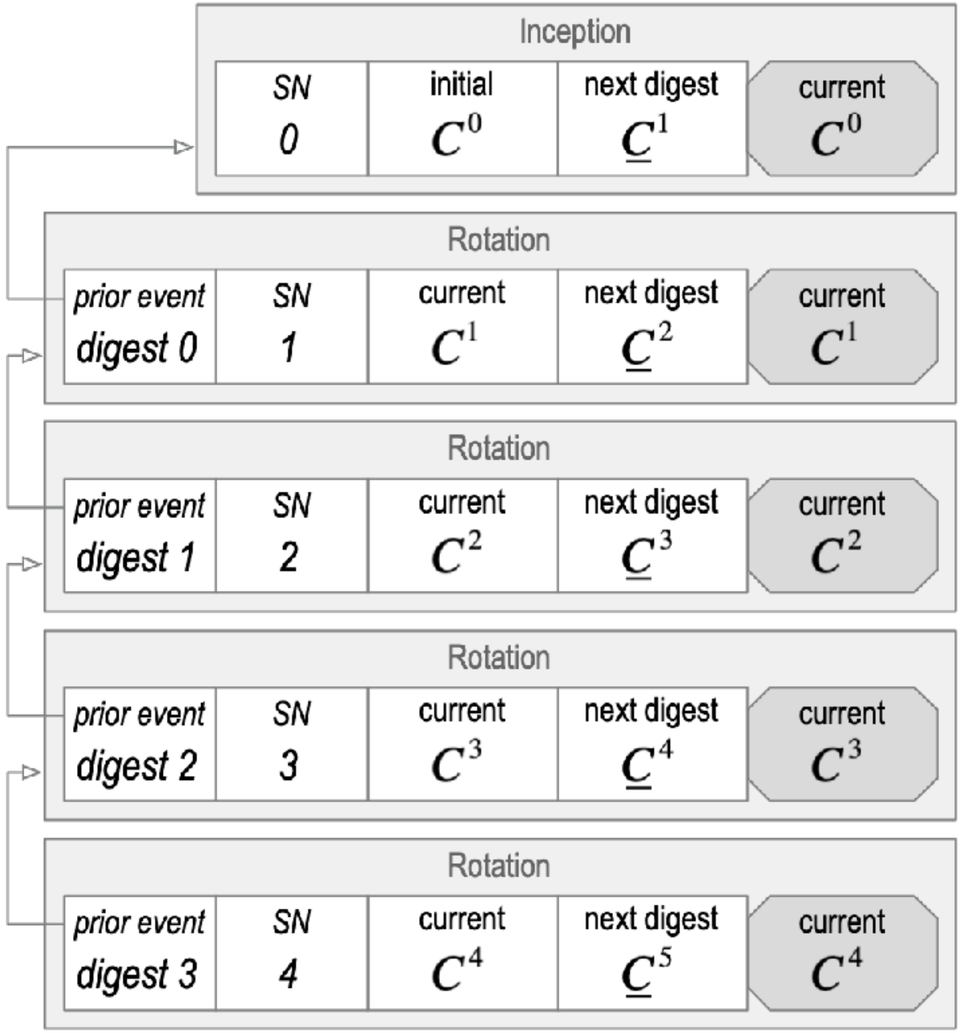
`EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148`

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

Solution: Key Pre-Rotation

duplicity evident
verifiable data
structure

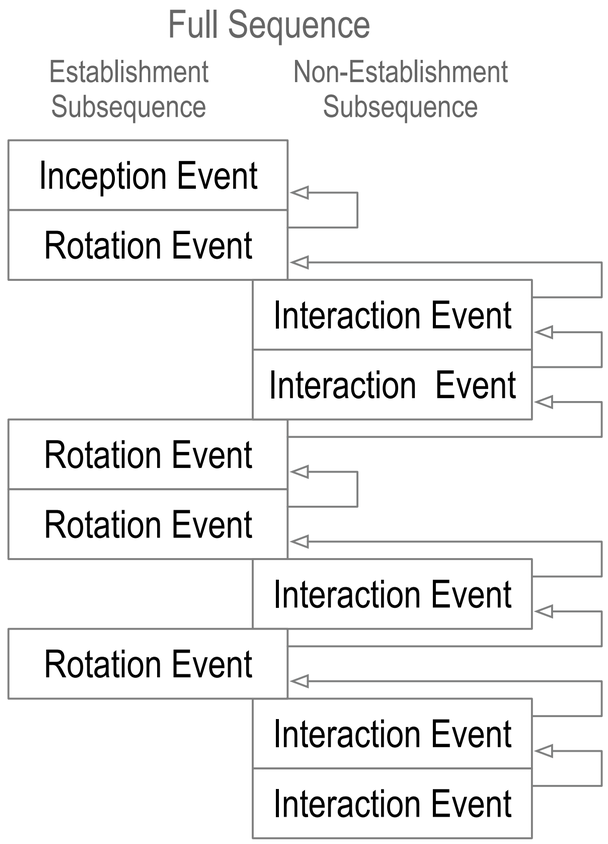




Digest of *next* key(s) makes pre-rotation post-quantum secure

D.J. Bernstein: https://cr.yp.to/hash/collisioncost-20090517.pdf

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

Duplicity Game

Cate promises to provide a consistent pair-wise log.

Local Consistency Guarantee

How may Cate be duplicitous and not get caught?

Cate
Controller
Log

A

Log V1 Log V2

B A

Log V2

Eve
Validator
Log

Joe
Validator
Log

private (one-to-one) interactions

Duplicity Game

Service promises to provide a consistent log to anyone.

Local Consistency Guarantee

How may Cate/Service/Agent be duplicitous and not get caught?

Cate
Controller
Log

Truncate Log

Delete Log

Service/Agent
Controlled by Cate
Log

A

Log V1 Log V2

B A

Log V2

Eve
Validator
Log

Joe
Validator
Log

highly available, private (one-to-one) interactions

Duplicity Game

Service promises to provide exact same log to everyone.

Global Consistency Guarantee

How may Cate and/or service be duplicitous and not get caught?

Cate
Controller
Log

Breaking the promise of global consistency is a provable liability.

Global consistency may only matter after Eve and Joe need to interact not before.

Service
Controlled by Cate
Log

Truncate Log

?

isolate network

isolate network

A

Delete Log

A

Doug
Global Duplicity
Log

log V1

log V2

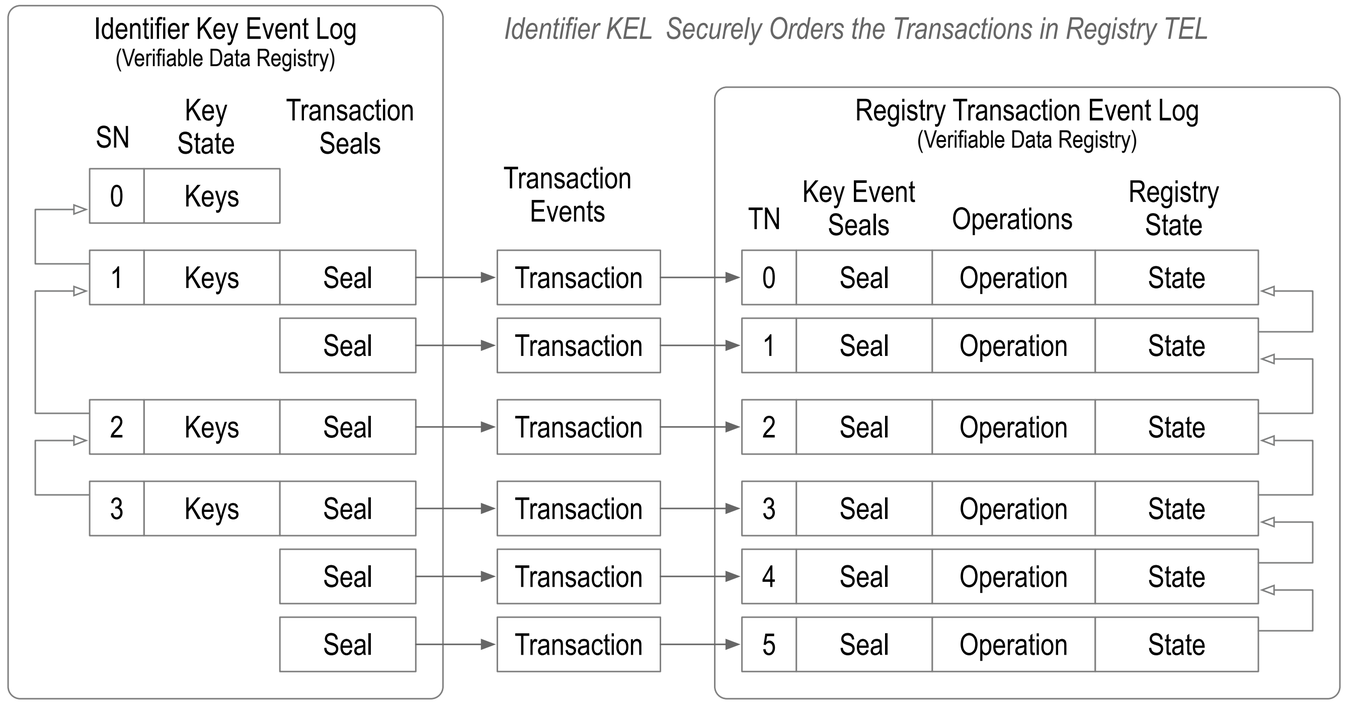
Eve
Validator
Log

Ambient Duplicity Detection

Joe
Validator
Log

global consistent, highly available, and public (one-to-any) interactions

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 KEL events.

Seals include cryptographic digest of external transaction data that binds the key-state of the anchoring event to the transaction event data anchored by the seal.

The set of transaction events that determine the external registry state form a log called a Transaction Event Log (TEL).

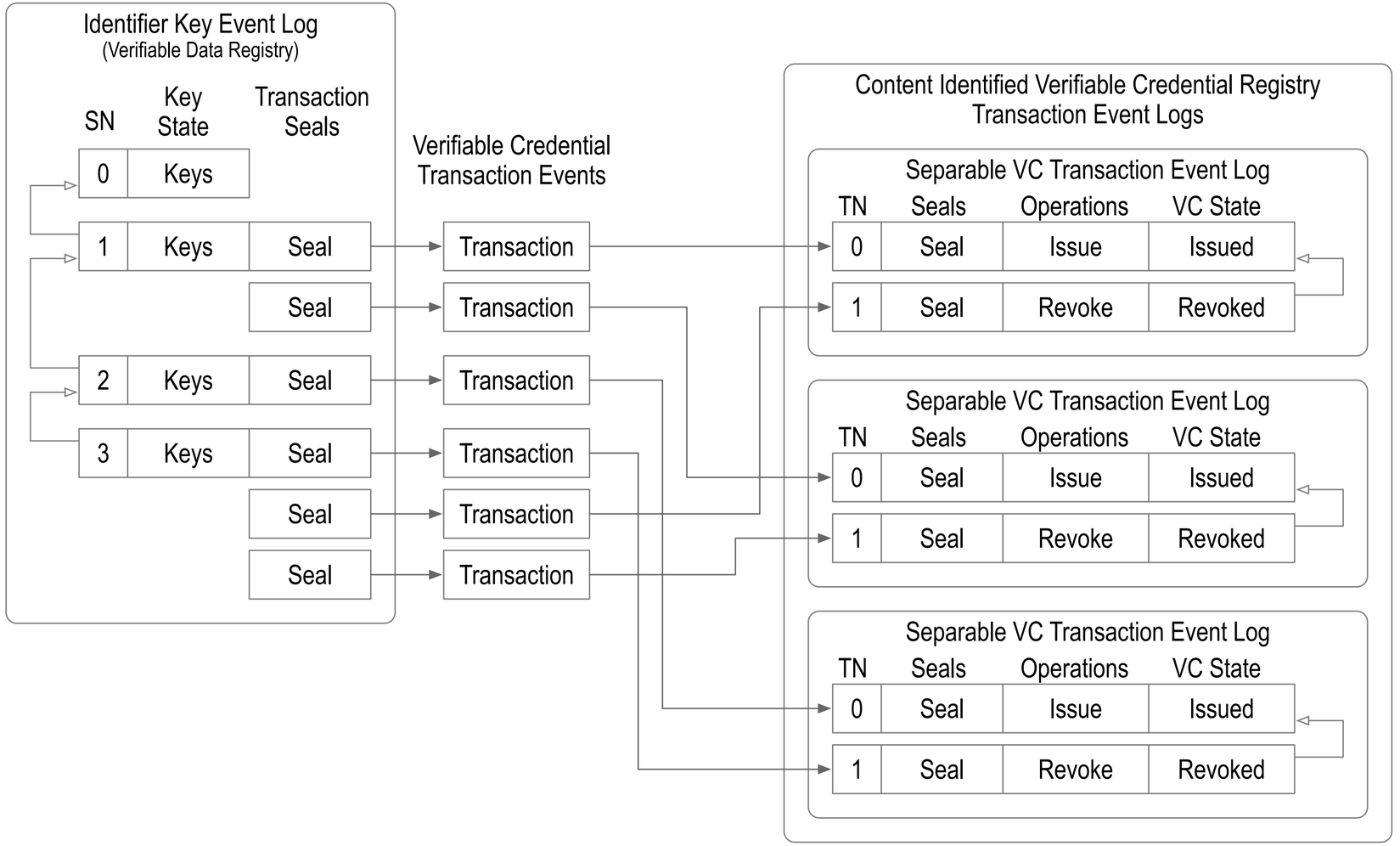
The transactions likewise contain a reference seal back to the key event authorizing the transaction.

This setup enables a KEL to control a TEL for any purpose. This includes what are commonly called “smart contracts”.

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

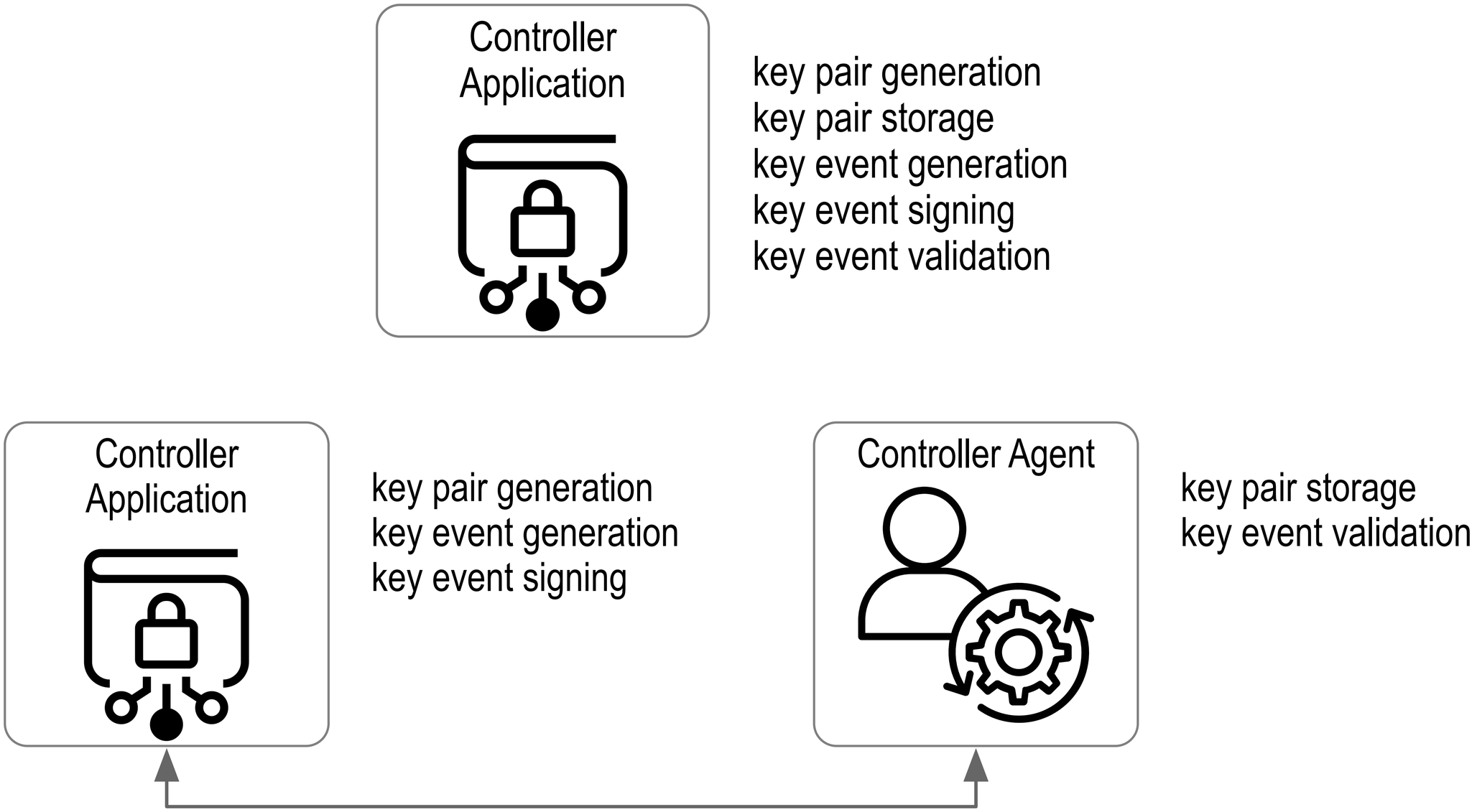
Any validator may therefore cryptographically verify the authoritative state of the registry.

KEL Anchored Issuance-Revocation Registry with Separable VC TELs



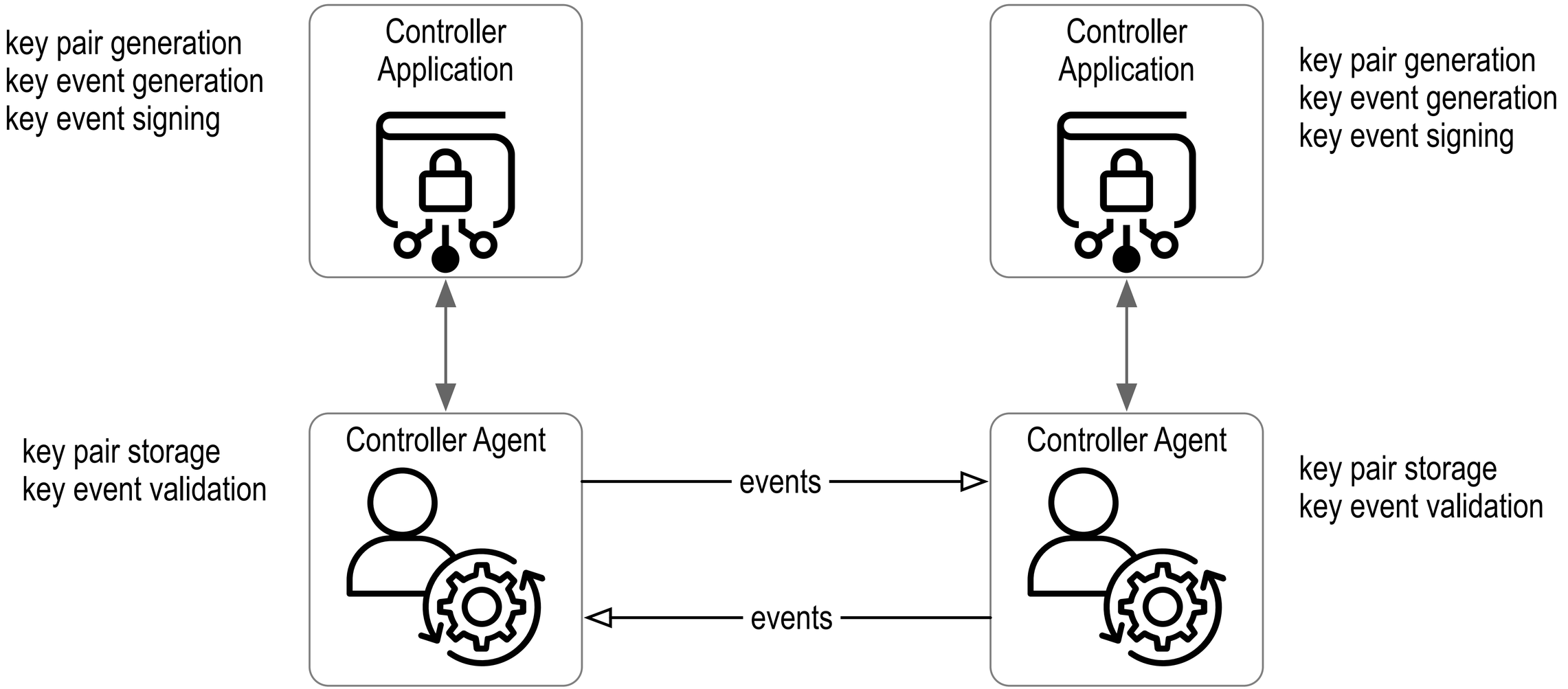
Each VC has a uniquely self-addressing identifier (SAID)
Each VC has a uniquely identified issuer (AID)
Each VC may have a uniquely identified issuee (AID).
All VC Schema are immutable

KERI Ecosystem Components: Controller Application and Agents

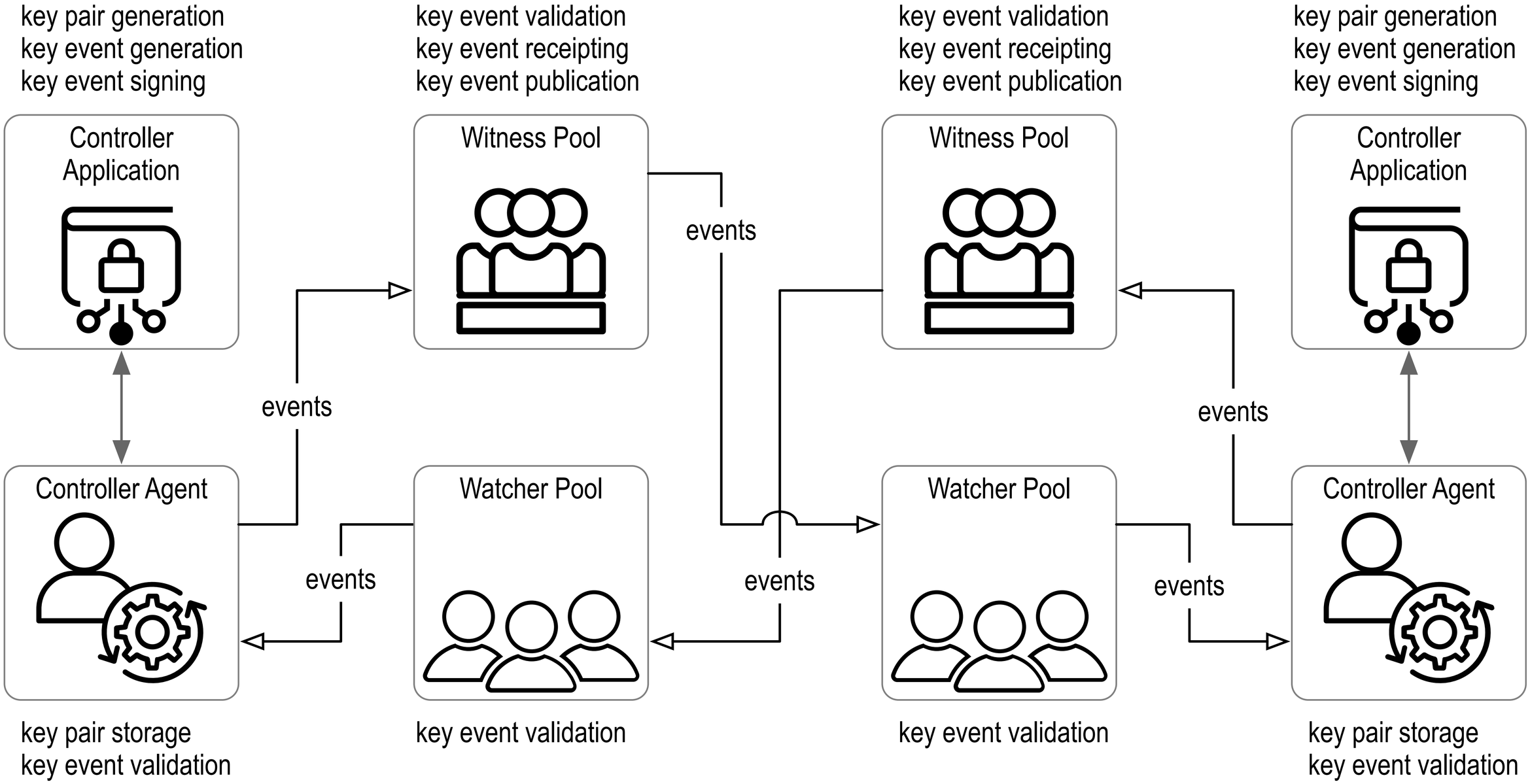


Modular, decentralized, web-based infrastructure without shared governance.

KERI Ecosystem Components: Peer-to-Peer Direct Mode

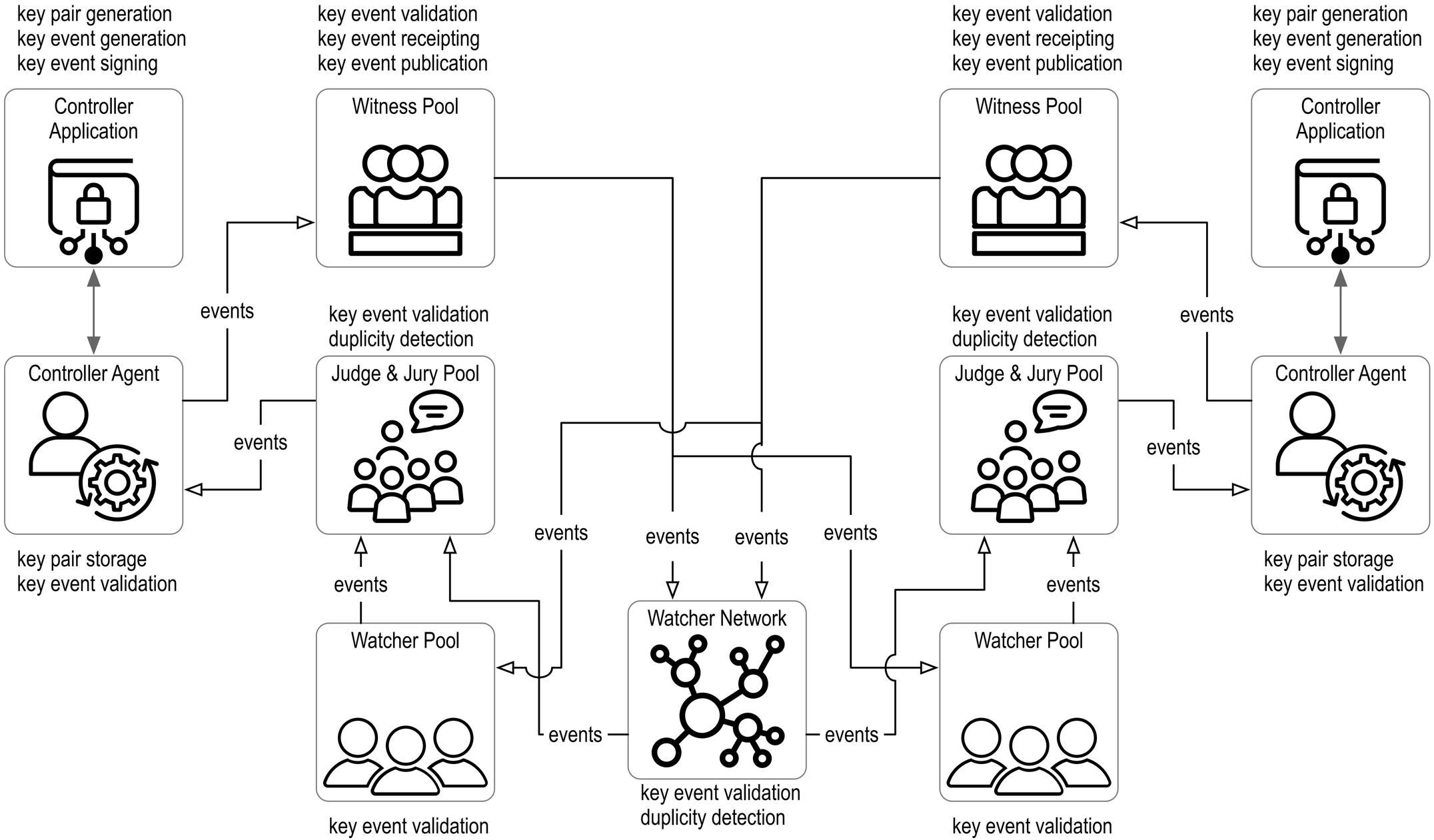


KERI Ecosystem Components: Witnesses and Watchers, Indirect Mode

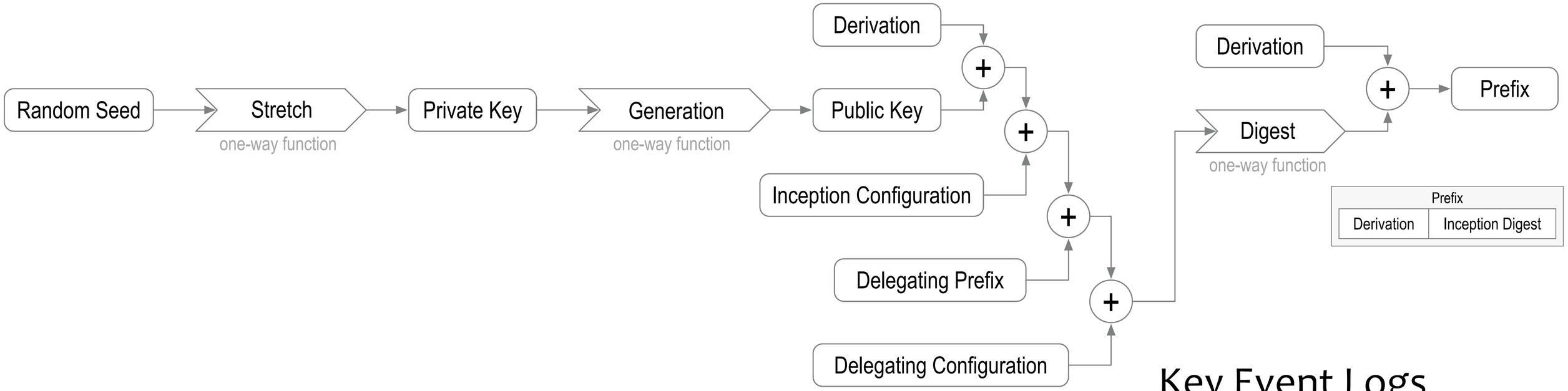


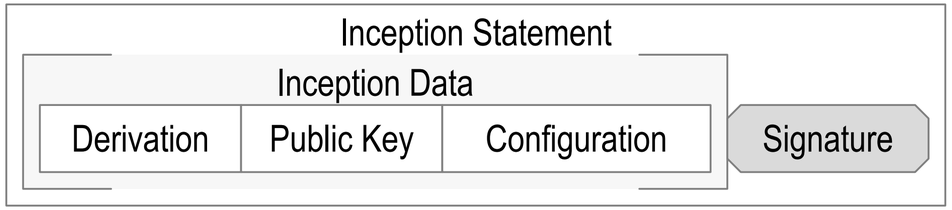
Modular decentralized web based infrastructure without shared governance

KERI Ecosystem Components: Witnesses and Watchers, Indirect Mode

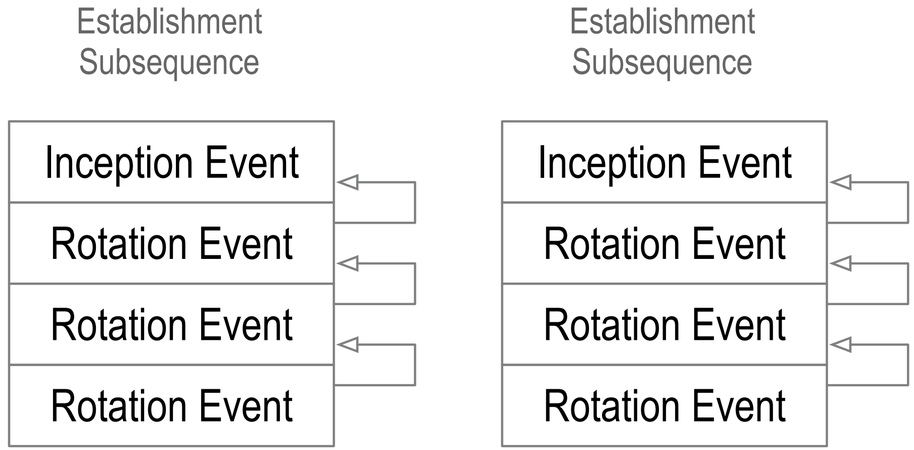


Delegated Identifiers





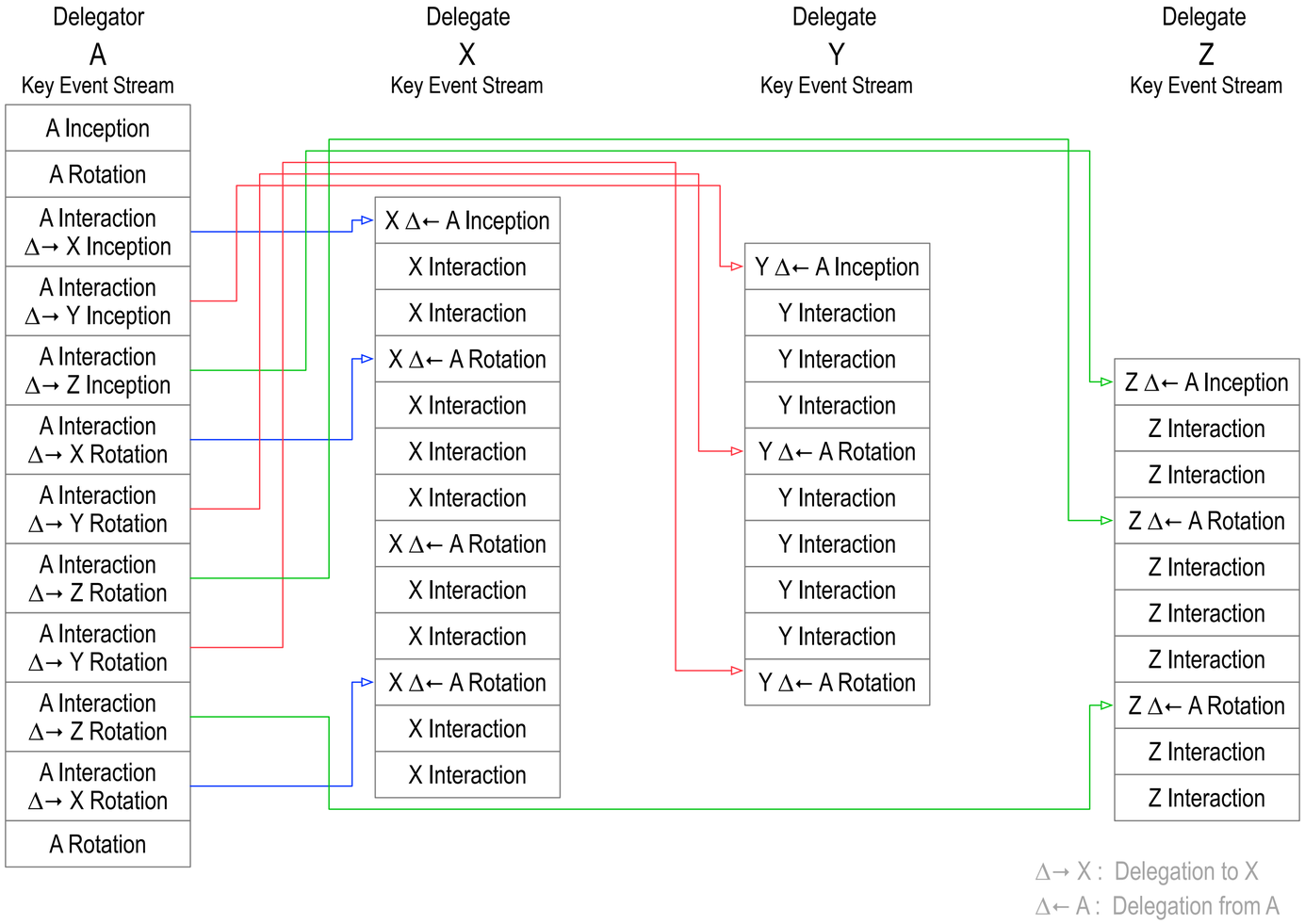
Key Event Logs

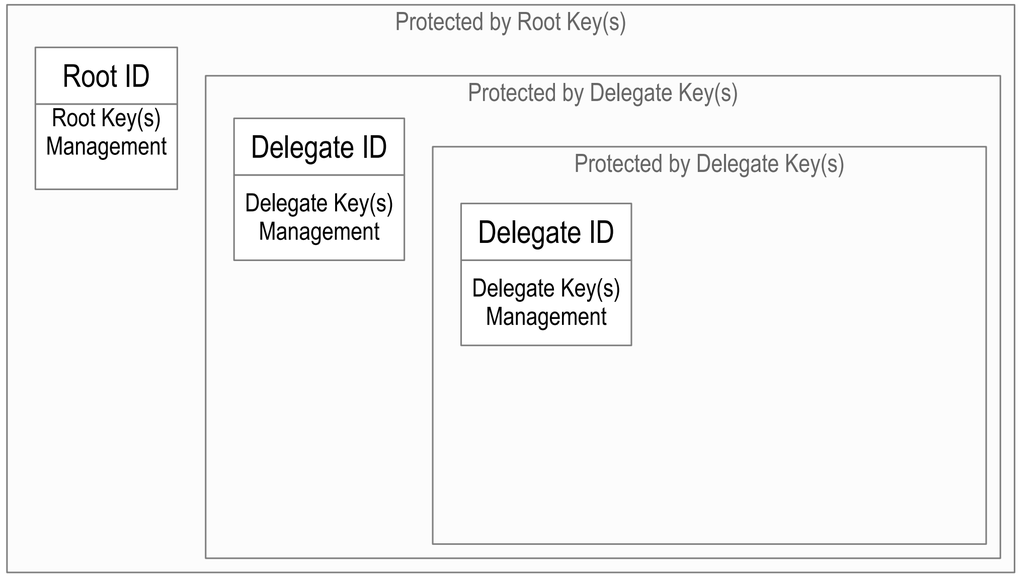


EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148

did:keri:EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148/path/to/resource?name=sec#yes

Identifier Delegation: Scaling & Protection





Hard Problems & Solutions

Moving Data Across Trust Domains.

No Shared Secrets

- No passwords
- No shared encryption keys
- No bearer tokens
- No shared private keys

Key Management (rotation)

True Zero-Trust = Sign Everything

Global Portability At-Scale

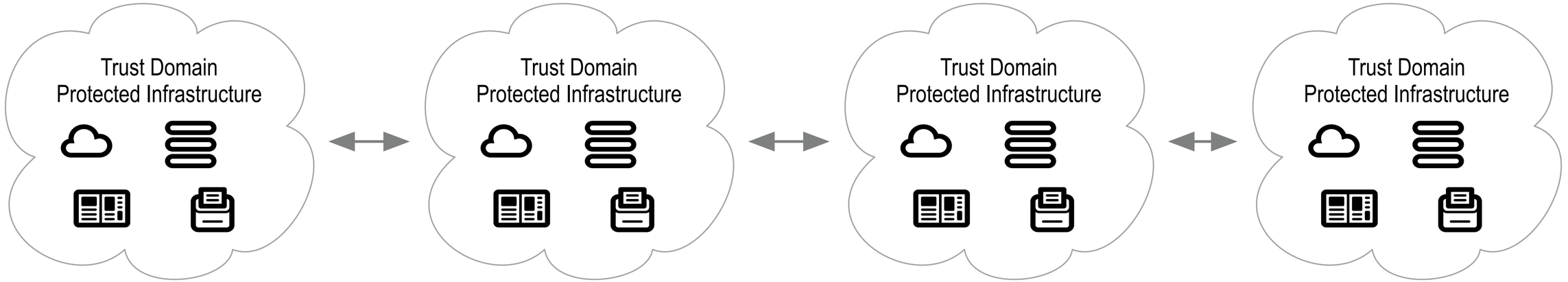
Trust Spanning Protocol (TSP)(SPAC)

Authentic Chained Data Container (ACDC)

Key Event Receipt Infrastructure (KERI)

Composable Event Streaming Representation (CESR)

GLEIF vLEI



Backup Slides