The Seven Privacies: Ugly Baby Pageant

The *privacy equivocation* mind virus

KERI

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

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

Resources

Resources:
https://keri.one/keri-resources/
KERI WebofTrust Community: (meetings, open source code Apache2, specification drafts)
https://github.com/WebOfTrust
https://github.com/WebOfTrust/keri
ToIP: (specifications OWF License) (New KERI Suite Working Group)
https://trustoverip.org/
https://wiki.trustoverip.org/display/HOME/ACDC+(Authentic+Chained+Data+Container)+Task+Force
https://trustoverip.github.io/tswg-cesr-specification/
https://trustoverip.github.io/tswg-keri-specification/
https://trustoverip.github.io/tswg-acdc-specification/
https://wiki.trustoverip.org/display/HOME/Trust+Spanning+Protocol+Task+Force
https://docs.google.com/document/d/1DsvAOGXlMFeE6tYlcaHlitoGLbWGfromRGrvR43zsgs/edit?tab=t.0
Adoptions:
GLEIF (ISO) vLEI: https://www.gleif.org/en/lei-solutions/gleifs-digital-strategy-for-the-lei/introducing-the-verifiable-lei-vlei
European Banking Authority
US Customs: webLEI/vLEI
healthKERI: https://healthkeri.com/
Provenant: https://provenant.net/
Kerion: https://kerion.one/

Equivocation

noun
the use of ambiguous language to conceal the truth or to avoid committing oneself; prevarication: I *say this without equivocation*.
Implies using words having more than one sense so as to seem to say one thing but intend another.
Words convey both meaning and emotion.
Emotional equivocation leverages the emotion of one sense to buttress a different sense.
Conveys a false impression.
Self-induced equivocation, believing your own hype.
Meaning trap.

Knowledge representation and *uncertainty*:
Likelihood, *imprecision*, and *ambiguity*.

Polysemy: same word; multiple related meanings. (form of ambiguity)
Ten most polysemous, single syllable words are: *cast (69), cut (63), draw (62), point (50), serve, strike,* and *through.*
Polysemous drift can be extreme enough to reach its own antonym:
to dust; remove particulates; add particulates
Hallucinations in LLMs are often the result of polysemy.
Undetectable attack on LLM is to inject phrases with high polysemous ambiguity.

Private (19)

adjective

- belonging to some particular person: *private property.*
- pertaining to or affecting a particular person or a small group of persons; individual; personal: *for your private satisfaction.*
- confined to or intended only for the persons immediately concerned; confidential: *a private meeting.*
- personal and not publicly expressed: *one's private feelings.*
- not holding public office or employment: *private citizens.*
- not of an official or public character; unrelated to one's official job or position: *a former senator who has returned to private life;*
  a college president speaking in his private capacity as a legal expert.
- removed from or out of public view or knowledge; secret: *private papers.*
- not open or accessible to the general public: *a private beach.*
- undertaken individually or personally: *private research.*
- without the presence of others; alone: *Let's go into another room where we can be private.*
- solitary; secluded: *He wants to meet us in a more private place.*
- preferring privacy; retiring: *a very private person.*
- intimate; most personal: *private behavior.*
- of, having, or receiving special hospital facilities, privileges, and services, especially a room of one's own and liberal visiting hours: *a private room;*
  a private patient.
- of lowest military rank.
- of, relating to, or coming from nongovernmental sources: *private funding.*

noun

- a soldier of one of the three lowest enlisted ranks.
- **privates.** private parts.

Idioms

- **in private**,
  not publicly; secretly: *The hearing will be conducted in private.*

Confidential (4)

adjective

- spoken, written, acted on, etc., in strict privacy or secrecy; secret: *a confidential remark.*
- indicating confidence or intimacy; imparting private matters: *a confidential tone of voice.*
- having another's trust or confidence; entrusted with secrets or private affairs: *a confidential secretary.*
- (of information, a document, etc.)
  - bearing the classification *confidential,* usually being above *restricted* and below *secret.*
  - limited to persons authorized to use information, documents, etc., so classified.
    Compare classification (def. 5).

Authentic (6)

adjective

- not false or copied; genuine; real: *an authentic antique.*
- having an origin supported by unquestionable evidence; authenticated; verified: *an authentic document of the Middle Ages; an authentic work of the old master.*
- representing one's true nature or beliefs; true to oneself or to the person identified: *a story told in the authentic voice of a Midwestern farmer; a senator's speech that sounded authentic.*
- entitled to acceptance or belief because of agreement with known facts or experience; reliable; trustworthy: *an authentic report on poverty in Africa.*
- *Law*.
  executed with all due formalities: *an authentic deed.*
- *Music*.
  - (of a church mode) having a range extending from the final to the octave above. Compare plagal.
  - (of a cadence) consisting of a dominant harmony followed by a tonic.

Why equivocation of the polysemous ambiguity of privacy is a mind virus!

The language we use *shapes* the way we think. We *can't think* of certain thoughts if we don't use *precise, unambiguous* meanings of words to convey those thoughts.

Lera Boroditsky

https://en.wikipedia.org/wiki/Lera_Boroditsky

https://www.ted.com/dubbing/lera_boroditsky_how_language_shapes_the_way_we_think/transcript?audio=en&language=en

Cultures that use languages without counting words, e.g. One, two, many, don't develop math.

When we abuse the concept of privacy by ascribing technology as privacy-preserving by equivocating on what "privacy" means, the result of using that technology is often the opposite of what was intended.

Using ***privacy*** as a sledgehammer to imbue technology with the emotion of privacy but without the actual qualities of privacy

PAC Theorem

An interaction between two parties may be two of the three, *private*, *authentic*, and *confidential* to the same degree, but not all three at the same degree.

Common Law Entick 1765

https://web.archive.org/web/20031021121842/http://www.constitution.org/trials/entick/entick_v_carrington.htm

“Papers are the owner’s goods and chattels: they are his ***dearest*** property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where ***private papers*** are removed and carried away, the ***secret nature*** of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.”

Supreme Court of the US describes Entick thusly:
"a 'great judgment', 'one of the landmarks of English liberty', 'one of the permanent monuments of the British Constitution', and a guide to an understanding of what the Framers meant in writing the Fourth Amendment".

Personal papers cannot be seized; private thought crimes (sedition libel)

US Law

4th and 5th amendments.

Boyd 1886 (unity of 4th and 5th amendments)
“Both amendments relate to the personal security of the citizen. They nearly run into, and mutually throw light upon, each other. When the thing forbidden in the Fifth Amendment, namely, compelling a man to be a witness against himself, is the object of a search and seizure of his private papers, it is an "unreasonable search and seizure" within the Fourth Amendment.”

US Law Continued

Katz 1967: Reasonable Expectation of Privacy; Non-content metadata vs content data.

Fisher: 1976: Separation of Fourth and Fifth Amendments. Subpoena power to collect evidence in any recorded form (not direct testimony). Personal private papers are no longer protected.
A court order to reveal secret keys to unlock data creates the "cruel trilemma" by forcing one to decide whether to 1) tell the truth and incriminate one's self, 2) lie and perjure one's self, or 3) refuse to answer and face contempt and jail.

FTC late 1990s: private data rights as consumer rights when promises of notice and consent with respect to shared data are violated (i.e. unfair trade practice).

Three Party Information Sharing and Leakage Model

Information is Shared between two parties.

Third party observers may obtain information:

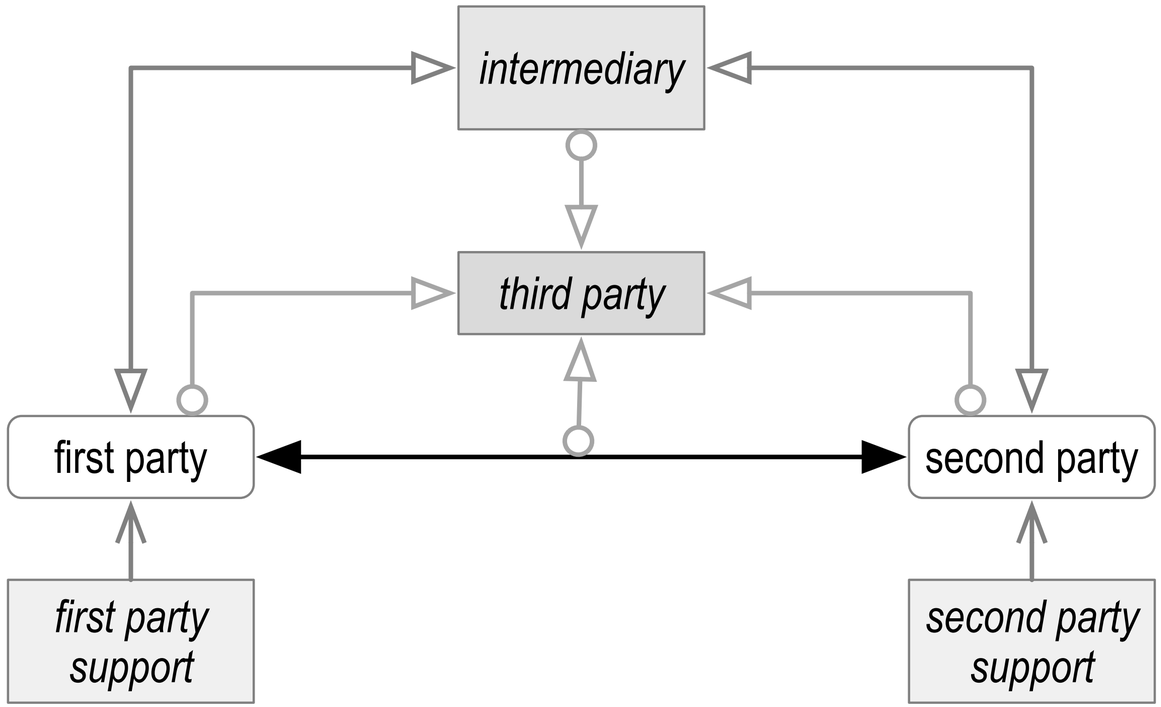
Indirectly as meta-data about the sharing interaction via leakage of the channel.

Directly from either of the first two parties and/or their supporting infrastructure including intermediaries.

Surveillance:

privacy is when third parties have no knowledge of ***who*** is sharing information

confidentiality is when third parties have no knowledge of ***what*** was shared.



Shared or not Shared; Secret or not Secret.

Information that is not-shared = private (one party data)

Information that is shared with restrictions = confidential (two party data, sensitive, protected)

Information that is shared without restrictions = non-confidential (any party data, public)

Surveillance

Non-content meta-data (unrestricted, information about the parties to the interaction)

Content data (confidential)

Content data is confidential, and meta-data about that content is not observable by third parties. (meta-data confidentiality, private network)

Combinations

not shared. (hiding, off-grid, air-gapped, physical possession, remote controlled)

shared but restricted i.e confidential (permissioned) (shared secret) sensitive protected

shared but not surveillable (meta-data and content)

shared de-identified but re-identifiable

shared cryptographically un-linkable but re-identifiable (unrestricted, surveillable, and correlatable)

shared but de-identified and non-re-identifiable: un-correlated, de-correlated, non-correlatable unlinked un-linkable.

private (not shared, not surveilled, and not identified)

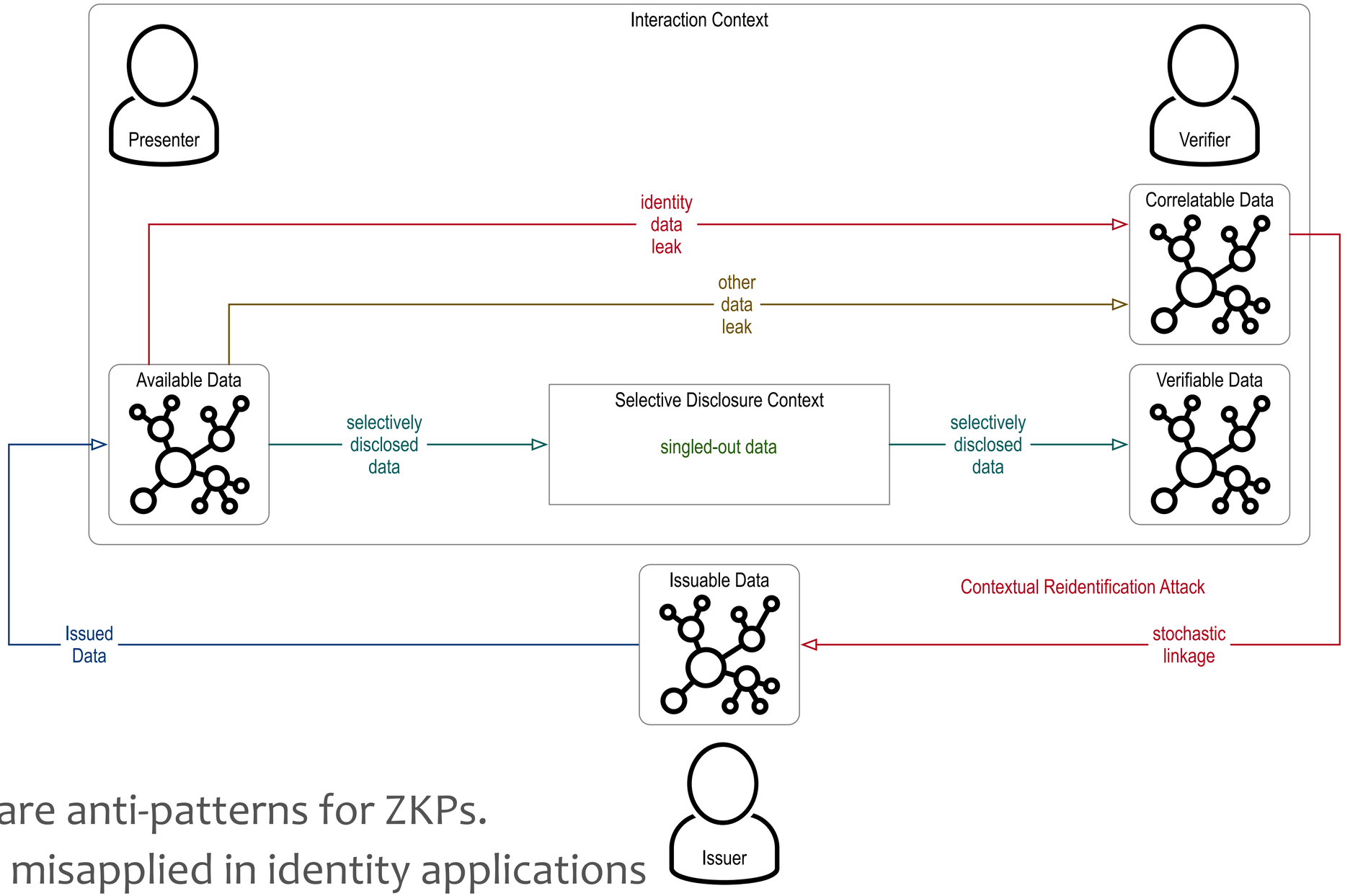
private keys

public keys

exposed secret keys (side-channel attacks)

shared secrets of all types (passwords, bearer tokens, passcodes, keys, DH exchanged keys, security questions. PII)

“*Hard*” privacy (*NOT*) with ZKPs



Leaky contexts are anti-patterns for ZKPs.

ZKPs are largely misapplied in identity applications

Interaction Contexts that defeat ZKP cryptographic unlinkability

Any interaction where the person is physically present at the time of presentation

Any interaction over a publicly routable network

Any virtual private network that does not route through a non-treaty country

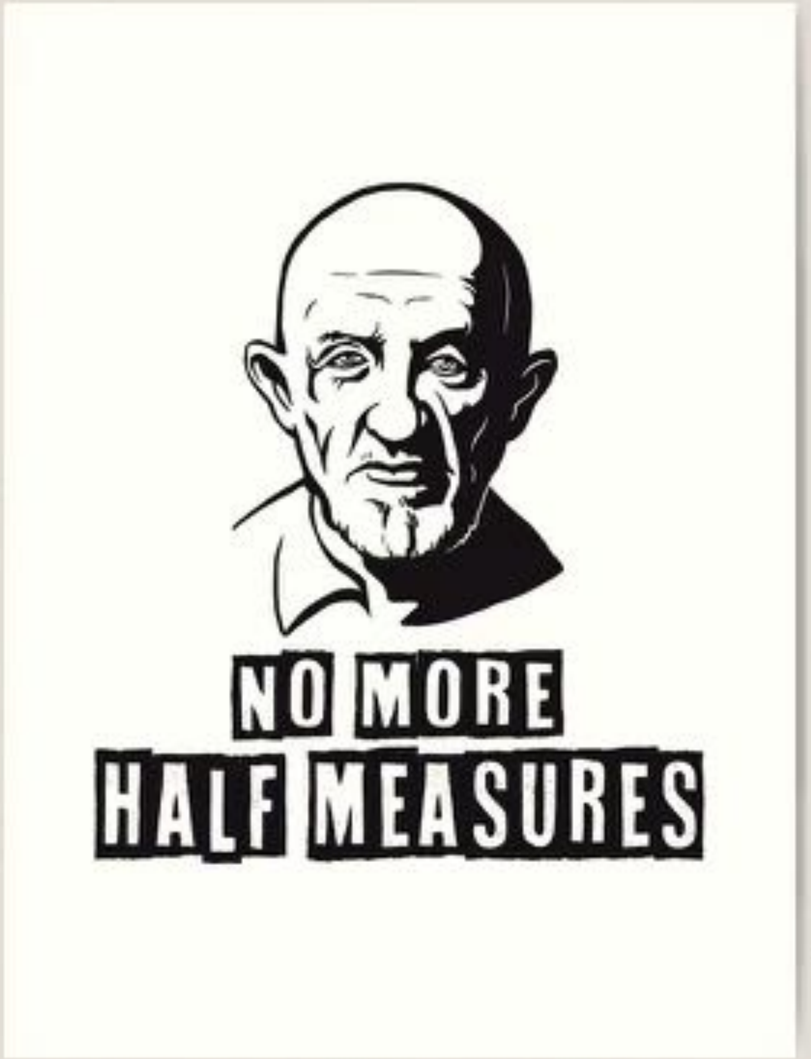
Any interaction that uses conventional payment rails

Any interaction that uses a conventional mobile phone

https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/SustainablePrivacy.pdf
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/SPAC_Message.pdf

Fallacy of argument that we should always start with crypto un-linkability as baseline

- Cryptographic unlinkability is not free. It forces hard tradeoffs.
- ZKPs in general are less secure that other mechanisms for selective disclosure. Detection of issuer key compromise requires breaking unlinkability.
- Insecurity increases the vulnerability of breach which increases the disclosure of data.
- It is easy to defeat in leaky interaction contexts, so bare crypto unlinkability is insufficient. It MUST require tight control over the interaction context, and the tight control must be compatible with the application adoption constraints. (no free lunch)
- The hard problem is not un-linkability but holding the 2nd party (verifier) accountable in order to ensure continued confidentiality of the selectively disclosed data.
- ZKP mechanisms defeat non-technological mechanisms for enforcing confidentiality.



Beware of half-measures that defeat full-measures

What is easily correlatable today is exponentially greater than what was correlatable 10 years ago, 5 years ago, 2 years ago

2024/01/24 Mother of all breaches (MOAB) 26 Billion Records: https://www.mcafee.com/blogs/internet-security/26-billion-records-released-the-mother-of-all-breaches/

2024/04/01 NDP Data Breach 2.9 Billion Records: https://npdbreach.com/

2024/02/01 Change Health Care Breach: 190 Million Records https://www.securitymagazine.com/articles/101340-190m-impacted-by-change-healthcare-breach-security-leaders-discuss

2023 Health Care Data Breaches 168 Million Records: https://www.hipaajournal.com/healthcare-data-breach-statistics/

Reach and Scope of Modern Data Aggregators:

ChatGPT4 = 1 PetaByte Training Data Set Size, not including all dynamically available data via connected agents.

Nation State Funded 5GW (Fifth Generation Warfare)

Corpus of personally linkable knowledge via re-identification attack

name, postal address(es), phone number(s), email address(es)

SSN, birthdate, age

biometrics: face, voice, DNA, fingerprints, gait

old passwords

any secrets previously used as shared AuthN factors

credit card numbers

credit history

medical history

anything from commercial background check, criminal history

text, email, social media

Google drive, MS Sharepoint drive

mobile GPS tracking data

surveillance data, security camera, ALPR etc

Any breached data of any kind

Anything scraped by LLM AI (ChatGPT, Gemini, Grok, etc)

Every act of Selective Disclosure contributes to this corpus of knowledge

The act of selective disclosure “singles-out” an individual thereby enabling correlation of the context of the act of disclosure to the corpus of knowledge about the individual. The selectively disclosed data along with the context of the act of disclosure is then added to this corpus of knowledge.

Therefore, counter-intuitively, selective disclosure increases the traceability of individuals, contradicting its falsely purported benefit of reducing the traceability.

The only individuals for whom this is not true are those that are “off-grid” or have fake identities

The only material benefit of selective disclosure is that the undisclosed information is not contributed to the corpus of knowledge, so it satisfies the principle of least disclosure, which reduces the rate at which the corpus of reidentifiable information grows over time.

Because the act of disclosure itself is sufficient to correlate that act to the corpus of knowledge that may be tracked/traced to the individual performing that act, the use of a cryptographic identifier in that disclosure is largely immaterial to the traceability of the act.

So whom or what does cryptographic “unlinkabililty” actually protect?

The flawed misconception of “unlinkability”

Unqualified “unlinkability” is impossible.

Every act in the defined use cases is easily *statistically contextually* ***linkable*** (correlatable) to the corpus of knowledge.

Qualified “cryptographic unlinkability" is a very ***weak*** form of unlinkability that actually defeats more comprehensive protection measures and increases traceability in the typical use cases.

The only unlinkability that matters is “contextual unlinkability,”

Given the extant corpus of knowledge, there is no technology that provides “contextual unlinkability”.

Therefore, providing “unlinkability” is not a viable policy goal.

Logical Entailment and Policy

A necessary condition means the consequent does not occur when the condition is absent.

A sufficient condition means the consequent must occur when the condition is present

A necessary condition appears as a subset of every sufficient condition

What are sufficient conditions for protecting an individual from tracking with respect to digital identity?

Is there a technology that provide a sufficient condition for protecting an individual from tracking?

Given a sufficient condition for protecting an individual from tracking does the addition of a given technology defeat that sufficient condition (i.e. does the technology itself make the sufficient condition insufficient)?

Can’t evaluate net benefit of any measure until we identify at least one sufficient measure.

Insufficient half-measure may defeat a sufficient full measure

What is the Policy Goal that defines sufficiency

The best that we can do?

The best we can do is a slippery slope. It is the rationale used to justify half-measures.

ZKPs and Selective Disclosure are justified as the best we can do, when indeed:

1) they are not the best we can do even only technologically

2) they are net counter productive

Suggested Policy Goal:

Exploitation of individuals wrt to tracking behavior by legitimate entities is protected such that on balance the expected cost of exploitation exceeds the expected benefit of exploitation.

How to achieve: Legal and regulatory measures coupled with technology that supports the legal and regulatory measures that in combination disincentivizes exploitation by legitimate entities.

Why crypto un-linkability is a self-defeating half-measure

- An anonymous party (with rare exceptions) is precluded from taking legal action against another party.
- Crypto Un-linkably disclosed data is unrestricted (permits re-identification and contextual linkage)
- 1st Parties need enforcement mechanisms (legal, regulatory, economic) facilitated by technology.
  - Contractually Protected Disclosure (ACDC Graduated Protected Selective Disclosure)
  - chain-link-confidentiality Hartzog 2012 https://scholarship.law.bu.edu/faculty_scholarship/3026/
  - Fiduciary Agents (AI)
  - Traceability of 1st party data within the infrastructure of the 2nd party
- The full-measure solution that best ensures continued confidentiality protection of shared data, including contextually leaked (surveilled) data/meta-data, requires a mixture of legal, regulatory, economic, and technical mechanisms.
- *Cryptographic un-linkability defeats legal, contractual, and economic accountability which are essential to solve the hard problem of contextual leakage!*

Sustainable Privacy

- https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/SustainablePrivacy.pdf
- Infrastructure that exhibits user data loyalty
- The myth of consent Solove 2024 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743
- Need data loyalty (fiduciary) mechanisms to protect the confidentiality of shared data (consent or not)
- User Delegated Fiduciary AI Agent Infrastructure
  - Enforcement requires at least latent accountability (i.e. latent linkability)
- Verifiable AI Algorithms and Infrastructure
  - Step 1 KERI (secure attribution is essential, but is defeated by unlinkability)
  - Step 2 …

Backup Slides

Protections in Three Party Information Sharing Model

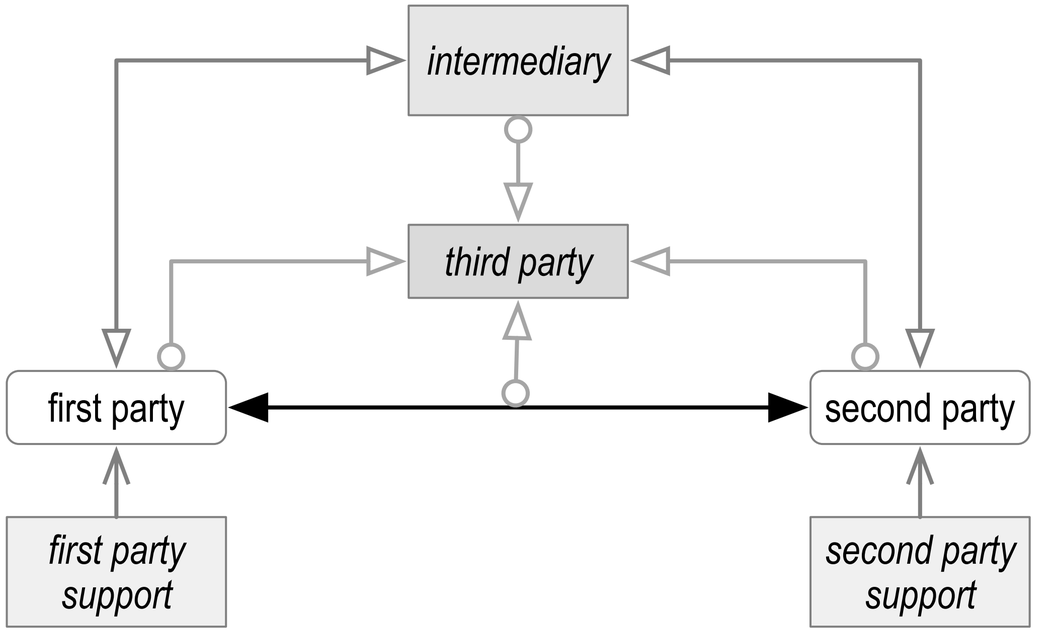
Privacy with respect to the 3rd party is protected if the 3rd party has no knowledge of the identifiers used by the 1st and 2nd parties for the conversation (disclosure).

Confidentiality with respect to the 3rd party is protected if the 3rd party has no knowledge of the disclosed data (the content data disclosed).

A 3rd party may directly break privacy by directly observing messages that contain the identifiers of the 1st and 2nd parties.

A 3rd party may directly break confidentiality by directly observing the content of messages between the 1st and 2nd parties.

The 3rd party may indirectly break both privacy and confidentiality by collusion with the 1st or 2nd party or via collusion with an intermediary.



US Law

4th and 5th amendments.

Boyd 1886 (unity of 4th and 5th amendments)

t“It does not require actual entry upon premises and search for and seizure of papers to constitute an unreasonable search and seizure within the meaning of the Fourth Amendment; a compulsory production of a party's private books and papers to be used against himself or his property in a criminal or penal proceeding, or for a forfeiture, is within the spirit and meaning of the Amendment.

It is equivalent to a compulsory production of papers to make the nonproduction of them a confession of the allegations which it is pretended they will prove.

A proceeding to forfeit a person's goods for an offence against the laws, though civil in form, and whether in rem or in personam, is a "criminal case" within the meaning of that part of the Fifth Amendment which declares that no person "shall be compelled, in any criminal case, to be a witness against himself."

The seizure or compulsory production of a man's private papers to be used in evidence against him is equivalent to compelling him to be a witness against himself, and, in a prosecution for a crime, penalty or forfeiture, is equally within the prohibition of the Fifth Amendment.

Both amendments relate to the personal security of the citizen. They nearly run into, and mutually throw light upon, each other. When the thing forbidden in the Fifth Amendment, namely, compelling a man to be a witness against himself, is the object of a search and seizure of his private papers, it is an "unreasonable search and seizure" within the Fourth Amendment.

Common Law Entick 1765

https://web.archive.org/web/20031021121842/http://www.constitution.org/trials/entick/entick_v_carrington.htm

Personal papers cannot be seized to prove private thought crimes (sedition libel).

Supreme Court of the US describes Entick thusly:
"a 'great judgment', 'one of the landmarks of English liberty', 'one of the permanent monuments of the British Constitution', and a guide to an understanding of what the Framers meant in writing the Fourth Amendment".

The messenger, under this warrant, is commanded to seize the person described, and to bring him with his papers to be examined before the secretary of state. In consequence of this, the house must be searched; the lock and doors of every room, box, or trunk must be broken open; all the papers and books without exception, if the warrant be executed according to its tenor, must be seized and carried away; for it is observable, that nothing is left either to the discretion or to the humanity of the officer. …

If it is law, it will be found in our books. If it is not to be found there, it is not law.
The great end, for which men entered into society, was to secure their property. That right is preserved sacred and incommunicable in all instances, where it has not been taken away or abridged by some public law for the good of the whole. The cases where this right of property is set aside by private law, are various. Distresses, executions, forfeitures, taxes etc are all of this description; wherein every man by common consent gives up that right, for the sake of justice and the general good. **By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing; which is proved by every declaration in trespass, where the defendant is called upon to answer for bruising the grass and even treading upon the soil. I**f he admits the fact, he is bound to show by way of justification, that some positive law has empowered or excused him. The justification is submitted to the judges, who are to look into the books; and if such a justification can be maintained by the text of the statute law, or by the principles of common law. If no excuse can be found or produced, the silence of the books is an authority against the defendant, and the plaintiff must have judgment.
According to this reasoning, it is now incumbent upon the defendants to show the law by which this seizure is warranted. If that cannot be done, it is a trespass.
Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.
…
I answer that the difference is apparent. In the one, I am permitted to seize my own goods, which are placed in the hands of a public officer, till the felon's conviction shall entitle me to restitution. In the other, the party's own property is seized before and without conviction, and he has no power to reclaim his goods, even after his innocence is cleared by acquittal.

Private (18)

adjective

: intended for or restricted to the use of a particular person, group, or class; a private park

: belonging to or concerning an individual person, company, or interest: a private house

: carried on by the individual independently of the usual institutions; a doctor in private practice

: being educated by independent study or a tutor or in a private school; private students

: restricted to the individual or arising independently of others; private opinion

: not general in effect; a private statute

: accommodating only one patient

: staying or recovering in a room accommodating only one patient.

: not related to one's official position

: PERSONAL private correspondence

: not holding public office or employment; a private citizen

: being a private

: not known or intended to be known publicly

: SECRET

: preferring to keep personal affairs to oneself

: valuing privacy highly

: withdrawn from company or observation; a private retreat

: unsuitable for public use or display

: not having shares that can be freely traded on the open market; a private company

noun

: an enlisted person of the lowest rank in the marine corps or of one of the two lowest ranks in the army

: a person of low rank in any of various organizations (such as a police or fire department)

: one not in public office

Confidential (4)

adjective

: intended for or restricted to the use of a particular person, group, or class

: PRIVATE, SECRET; confidential information.

: containing information whose unauthorized disclosure could be prejudicial to the national interest; compare SECRET, TOP SECRET

: marked by intimacy or willingness to confide; a confidential tone

: entrusted with confidences; a confidential clerk

Privacy (5)

noun

: the quality or state of being apart from company or observation

: SECLUSION

: freedom from unauthorized intrusion; one's right to privacy

: SECRECY

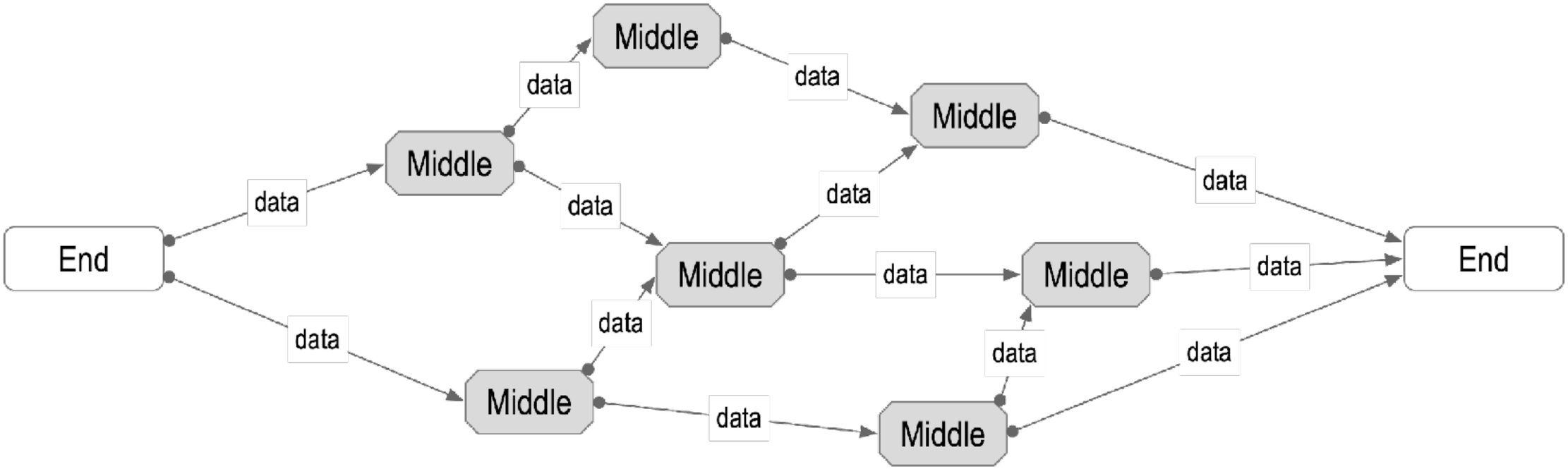
: a private matter

: SECRET

: a place of seclusion

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

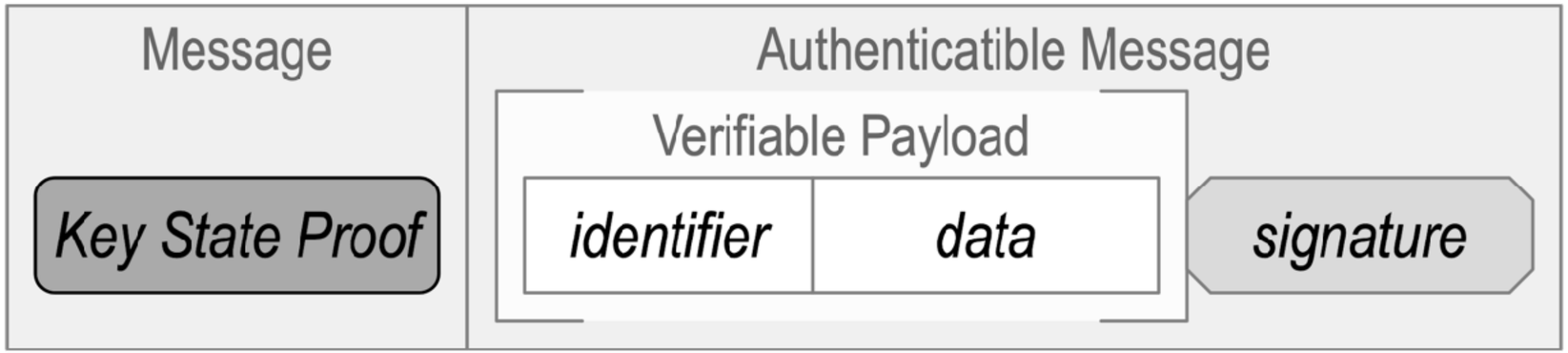
Zero-Trust-Computing

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

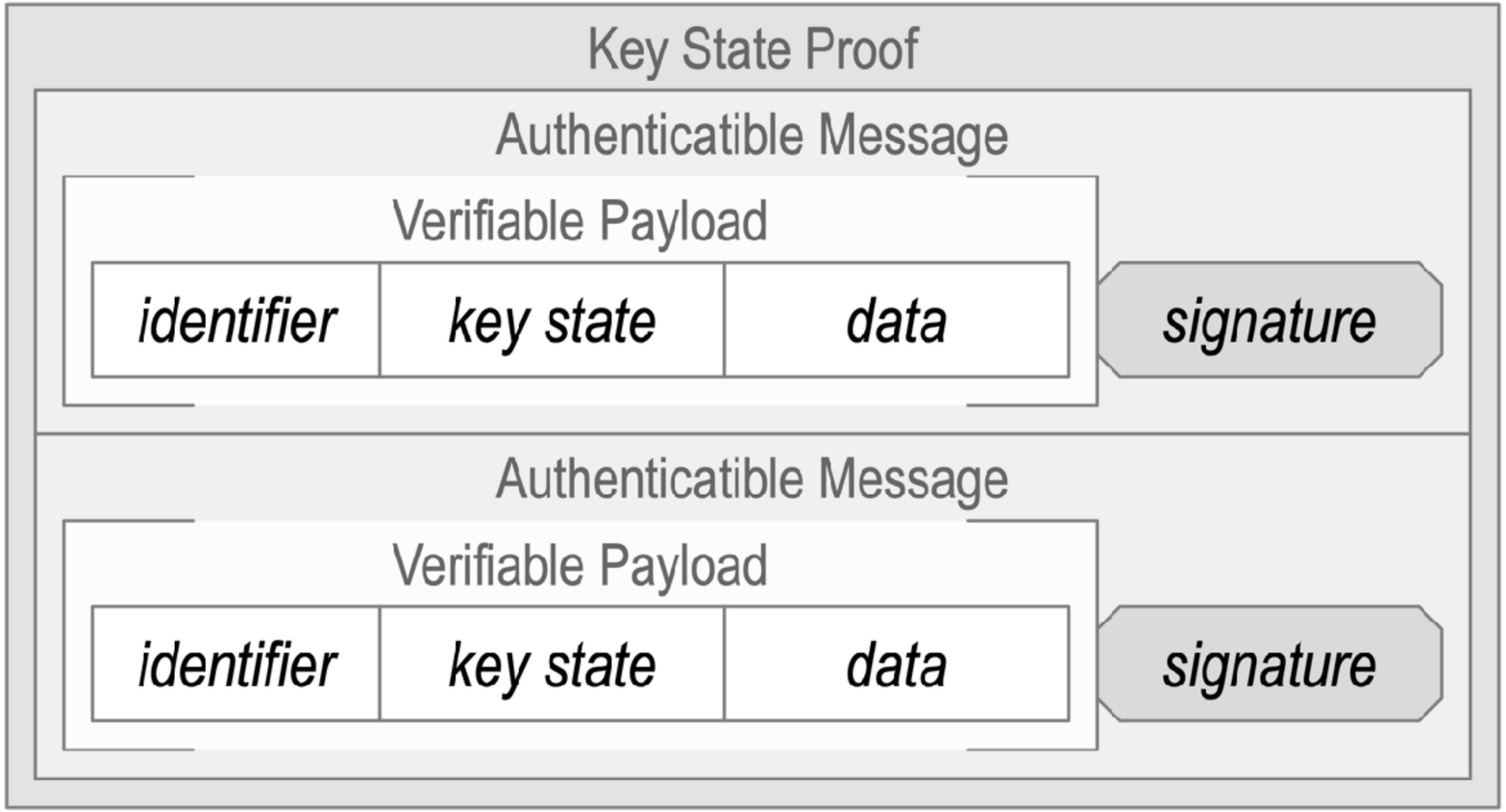
Establish authenticity of IP packet's message payload.



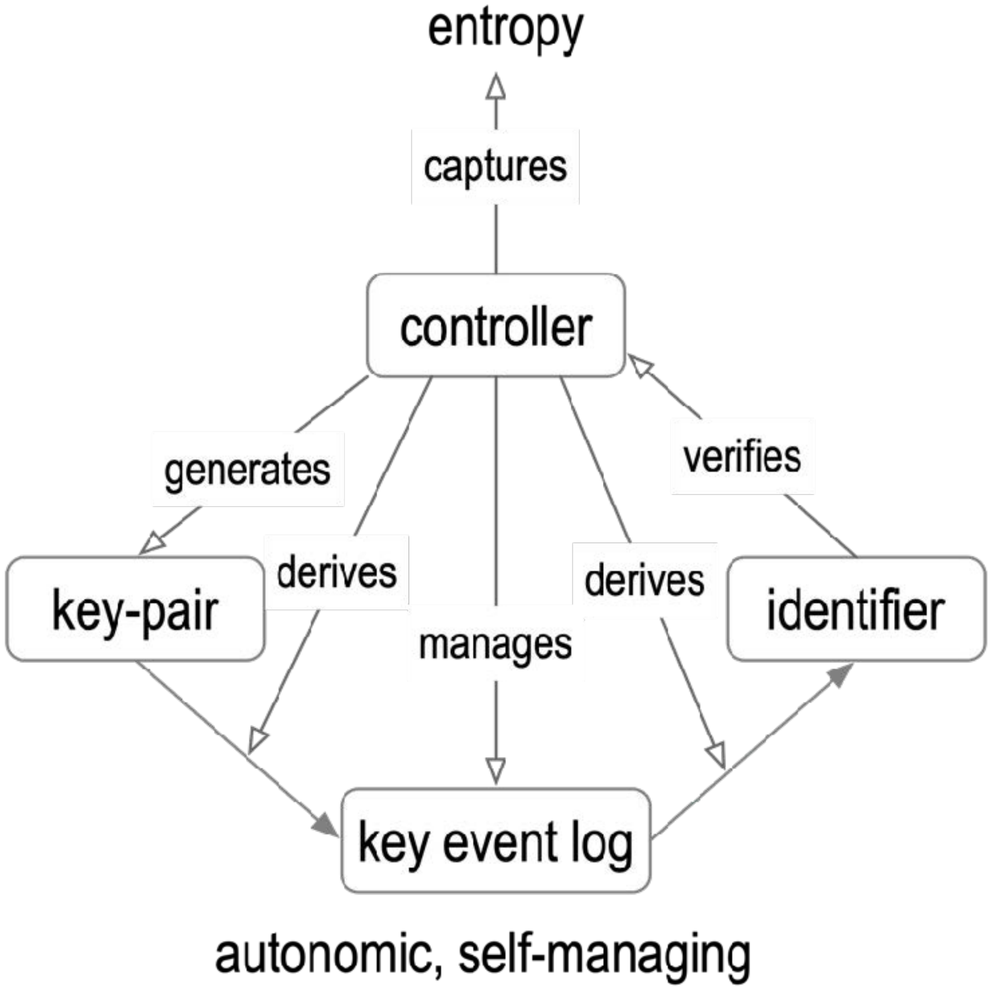
The overlay's security is contingent on the mapping's security.

Key State Proof is Recursive Application of Overlay

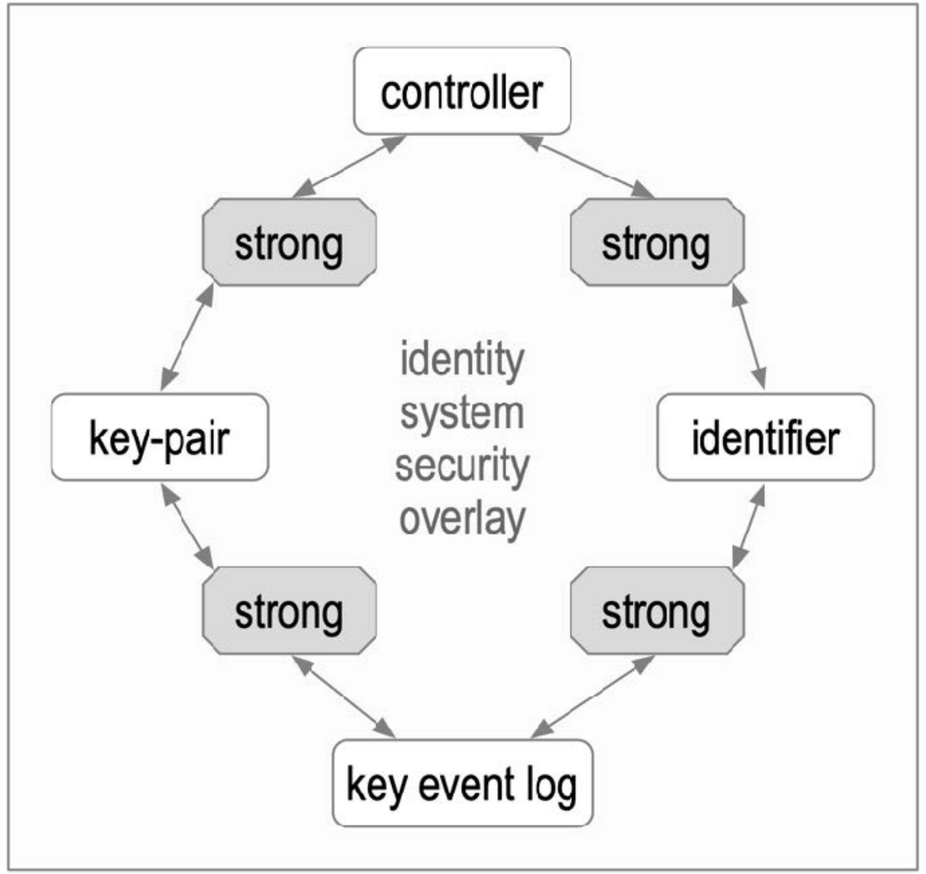
Persistent mapping via verifiable data structure of key state changes



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



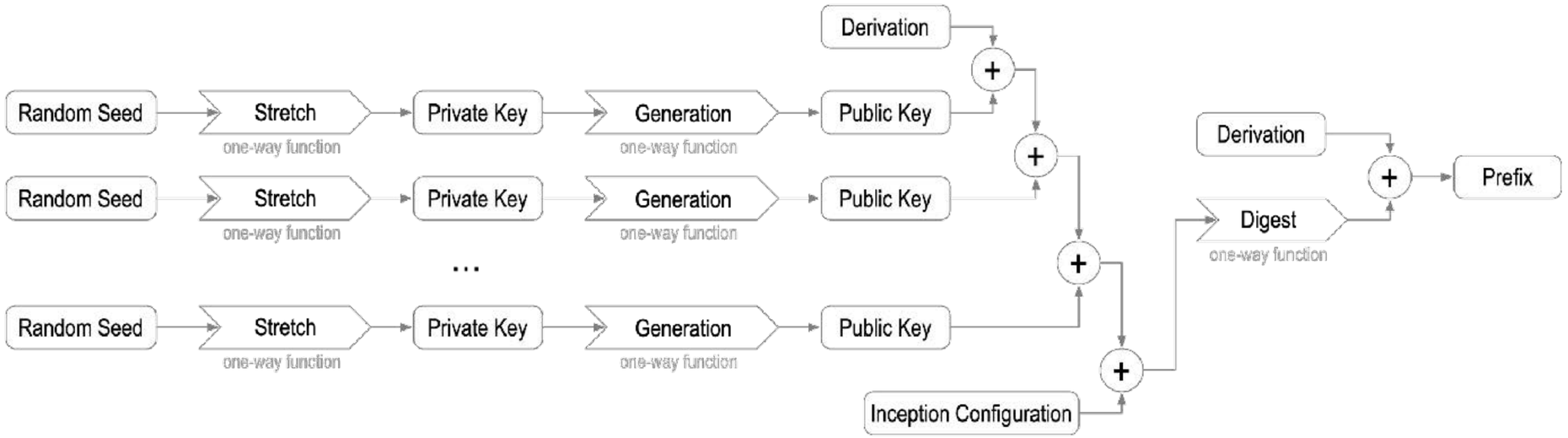
autonomic, self-managing

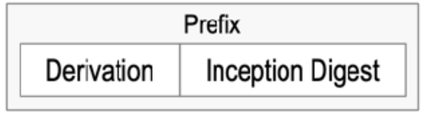


Autonomic Identifier Issuance Tetrad

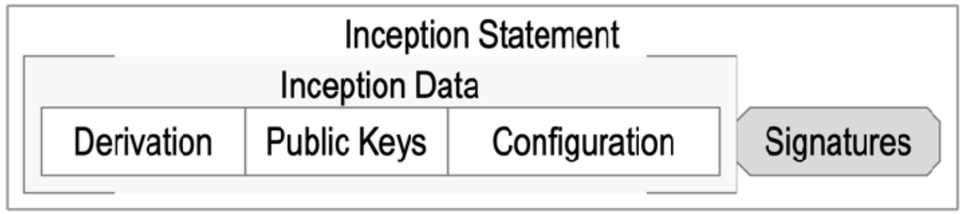
cryptographic root-of-trust with verifiable persistent control

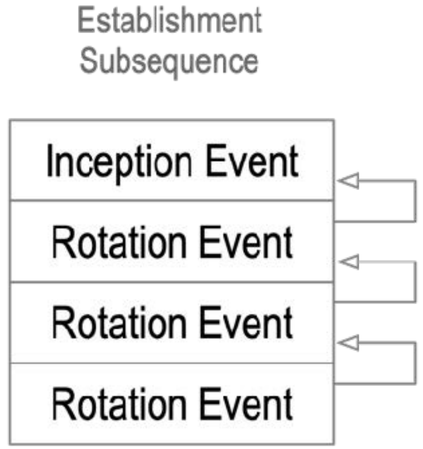
Cryptographic Root-of-Trust:
Self-Certifying Identifier (SCID) + Key Event Log = Autonomic Identifier (AID)





Key Event Log



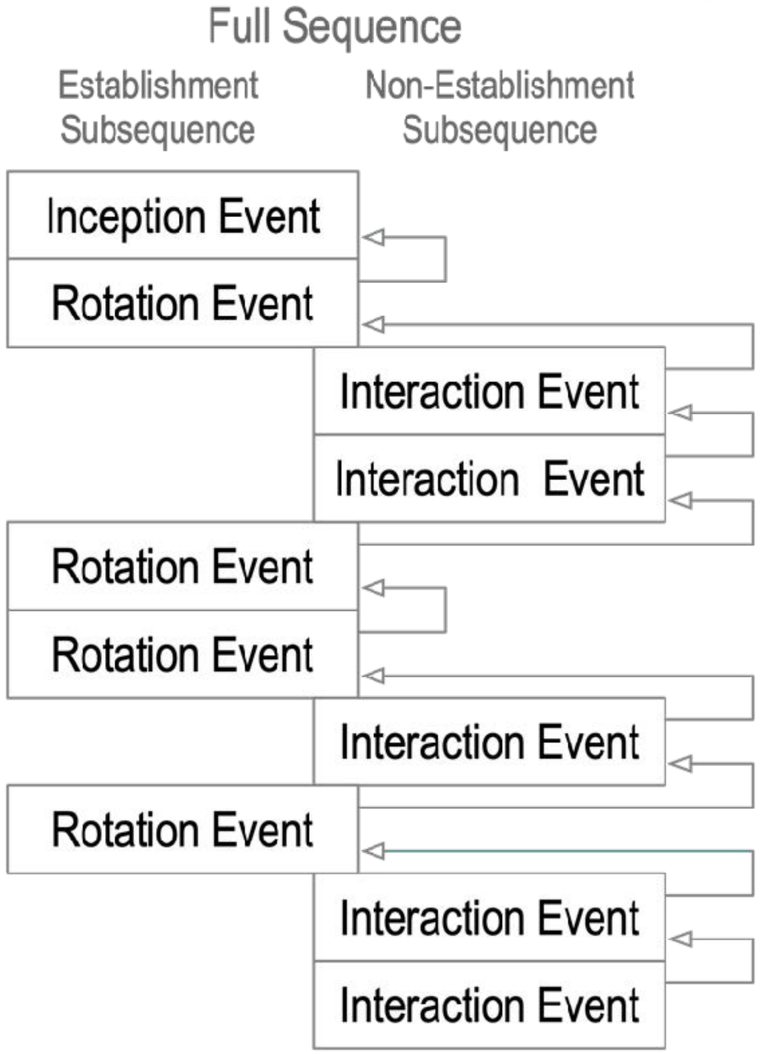


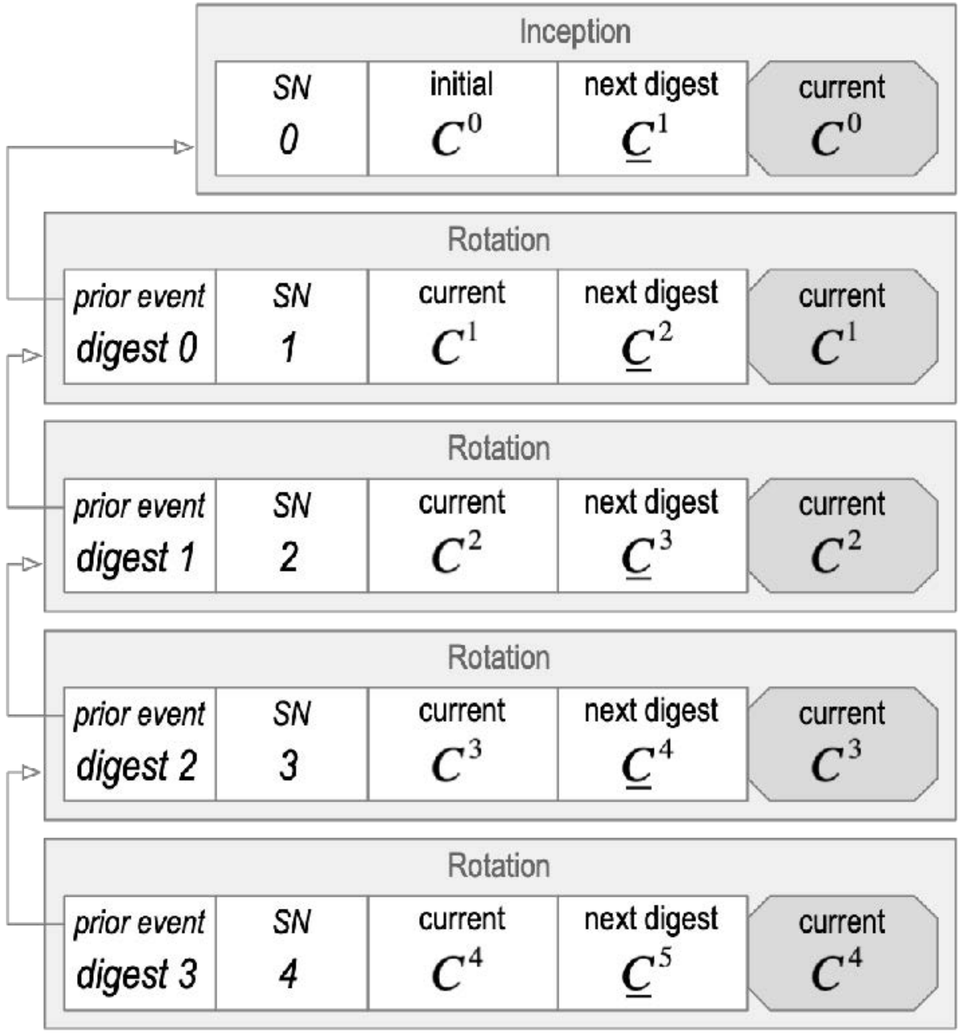
`EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148`

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

Solution: Key Pre-Rotation

duplicity evident
verifiable data
structure

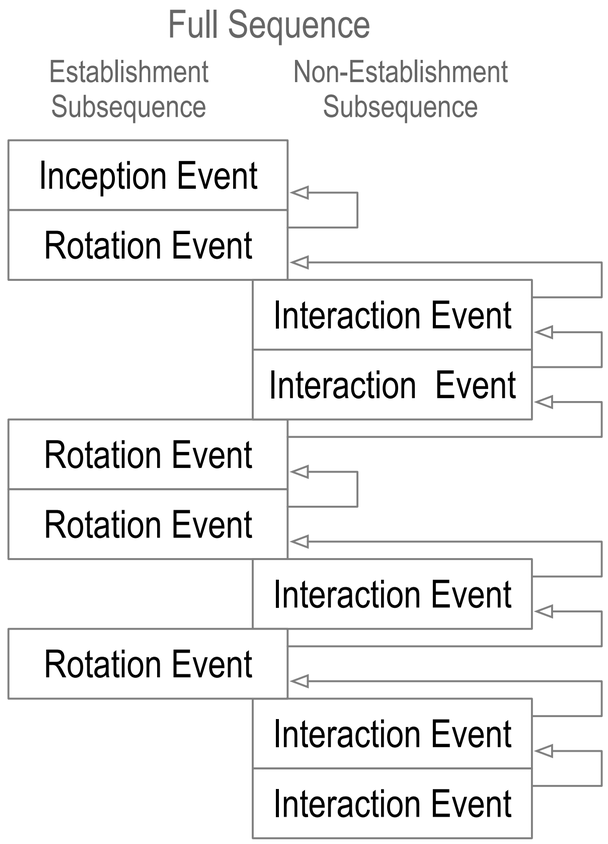




Digest of *next* key(s) makes pre-rotation post-quantum secure

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

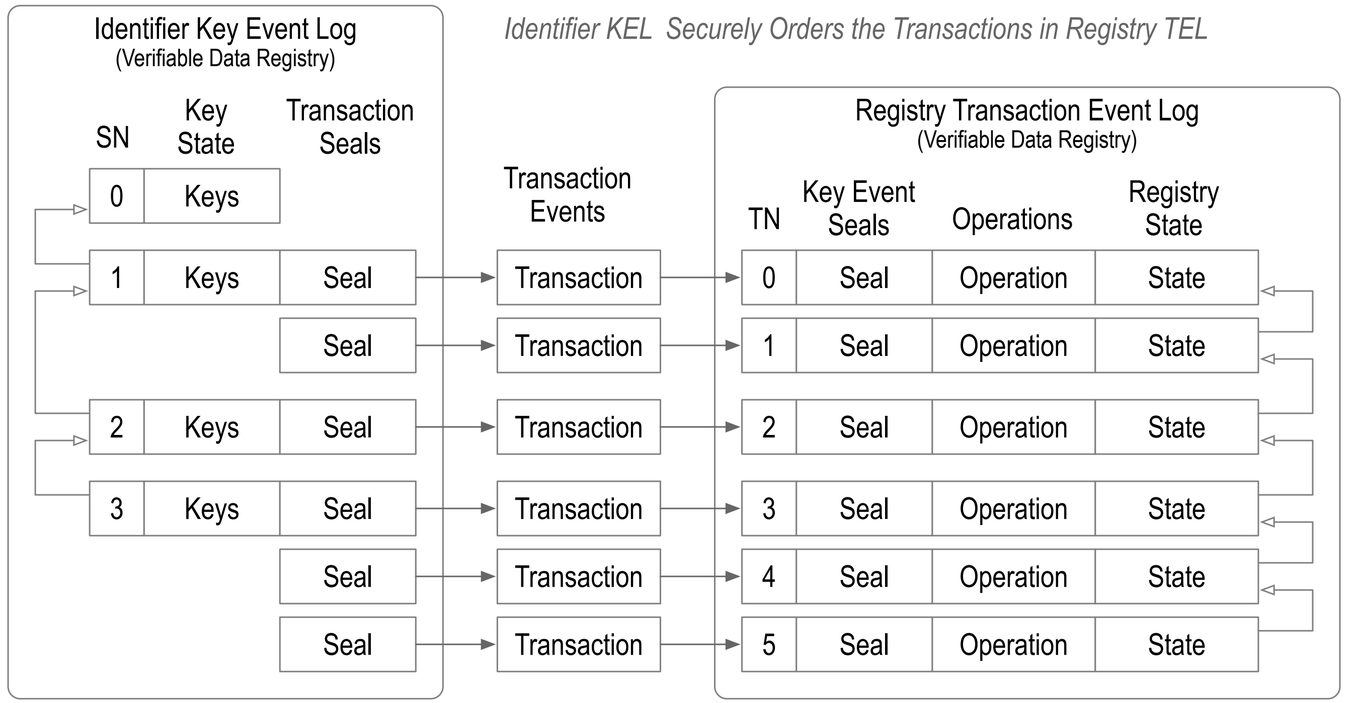
Eve
Validator
Log

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).

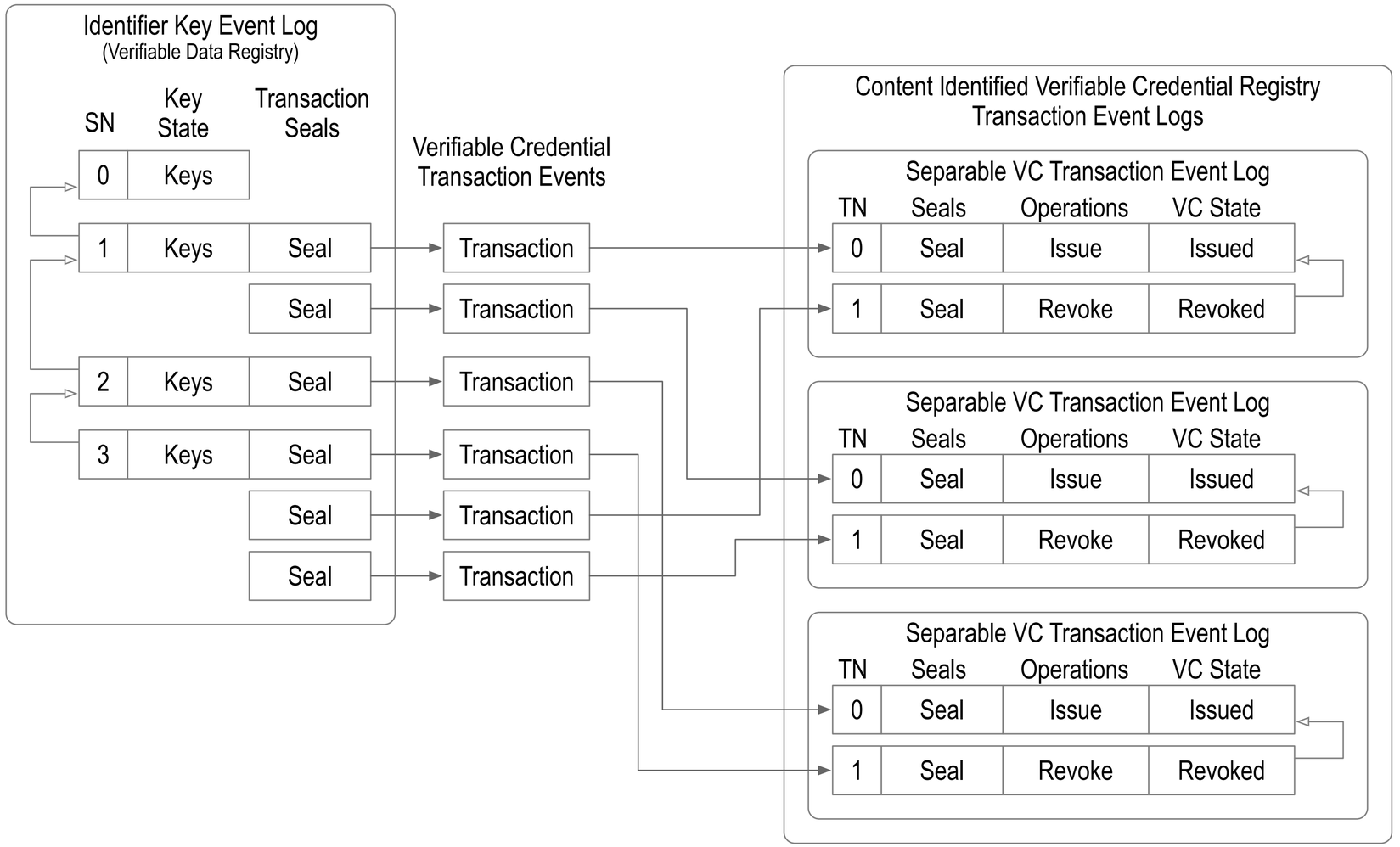
The transactions likewise contain a reference seal back to the key event authorizing the transaction.

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.

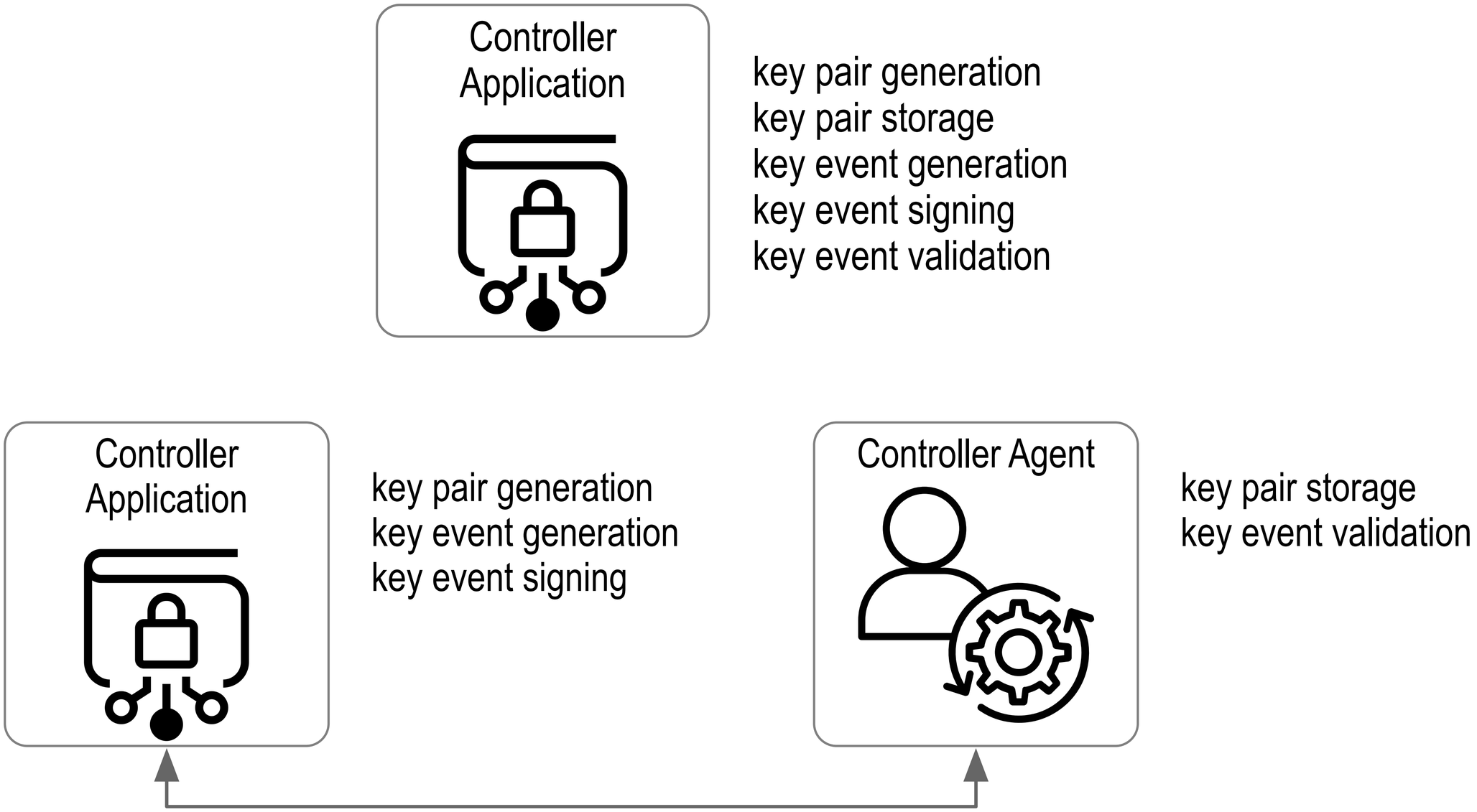
Any validator may therefore cryptographically verify the authoritative state of the registry.

KEL Anchored Issuance-Revocation Registry with Separable VC TELs



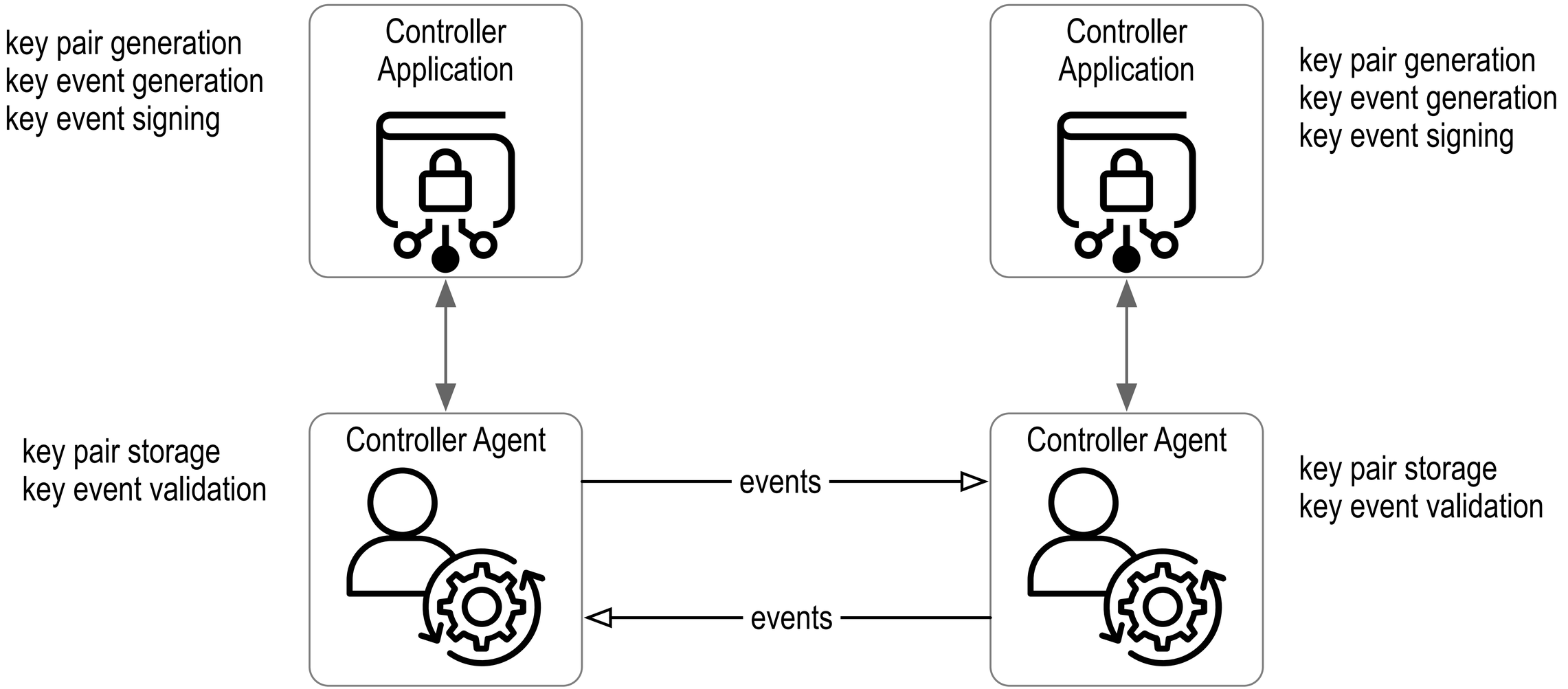
Each VC has a uniquely self-addressing identifier (SAID)
Each VC has a uniquely identified issuer (AID)
Each VC may have a uniquely identified issuee (AID).
All VC Schema are immutable

KERI Ecosystem Components: Controller Application and Agents

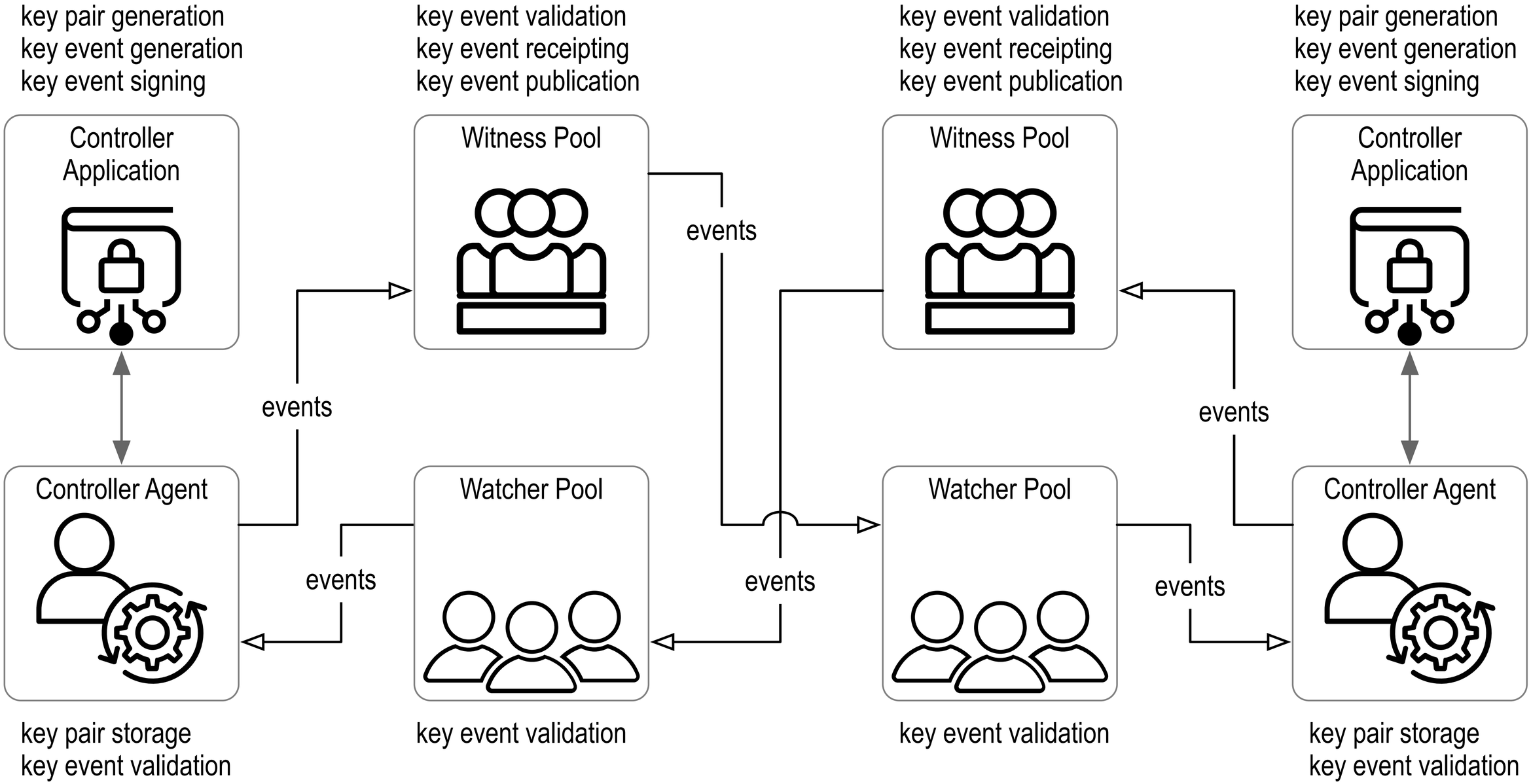


Modular, decentralized, web-based infrastructure without shared governance.

KERI Ecosystem Components: Peer-to-Peer Direct Mode

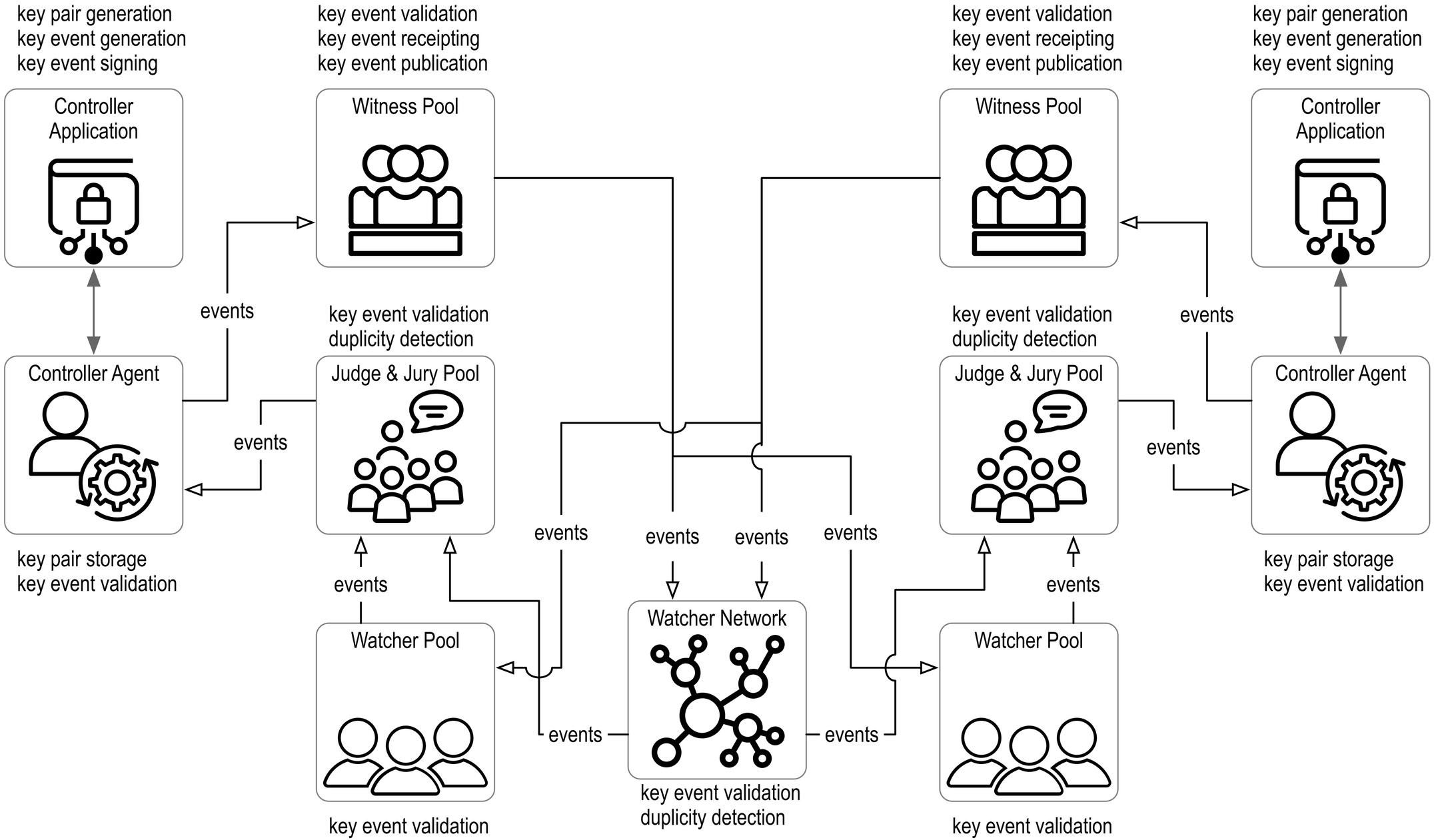


KERI Ecosystem Components: Witnesses and Watchers, Indirect Mode

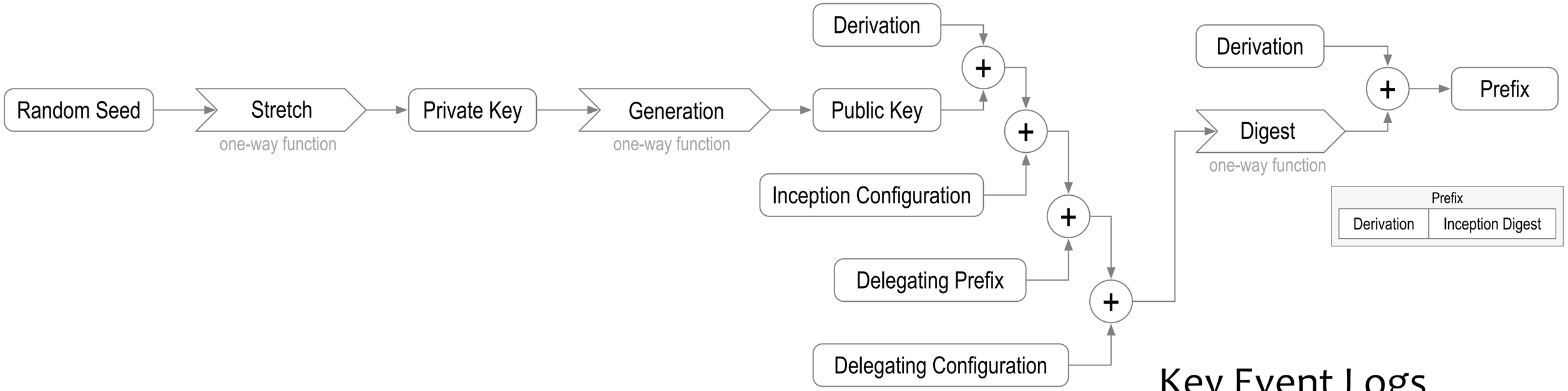


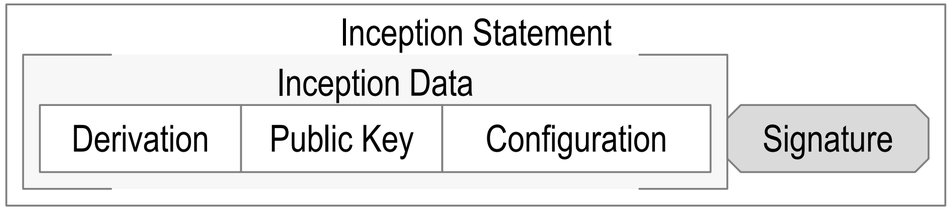
Modular decentralized web based infrastructure without shared governance

KERI Ecosystem Components: Witnesses and Watchers, Indirect Mode

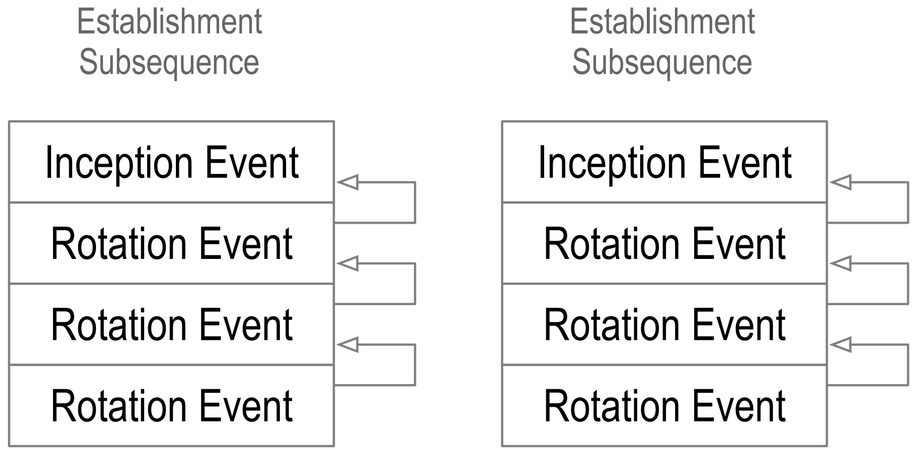


Delegated Identifiers





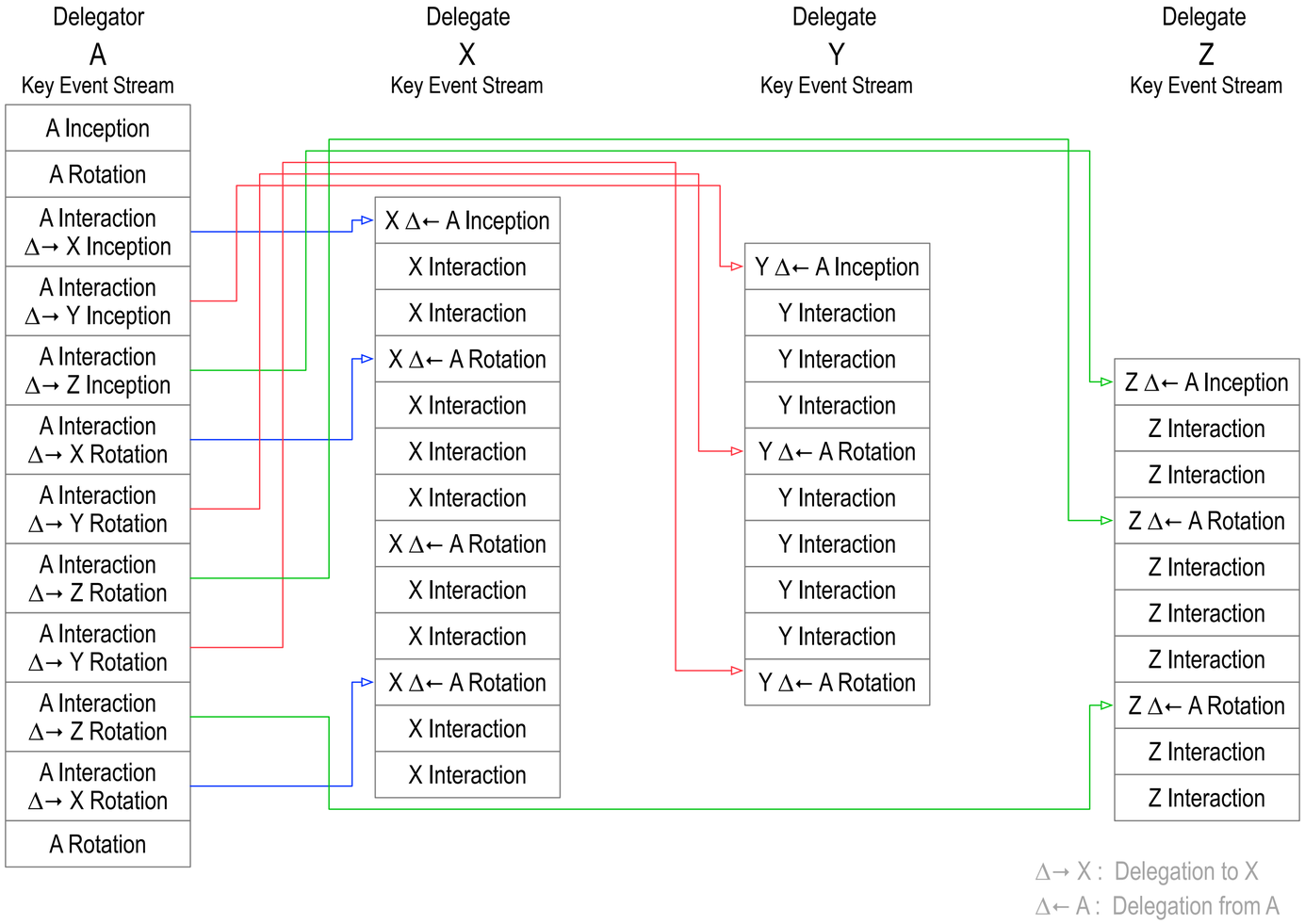
Key Event Logs

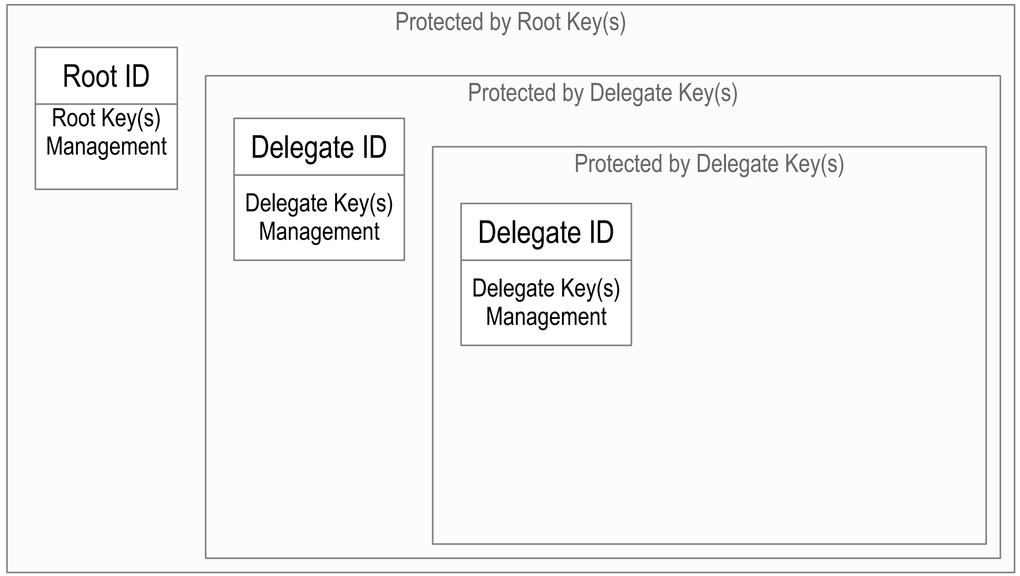


EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148

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