SEDI

Policy and Technology Trade Space

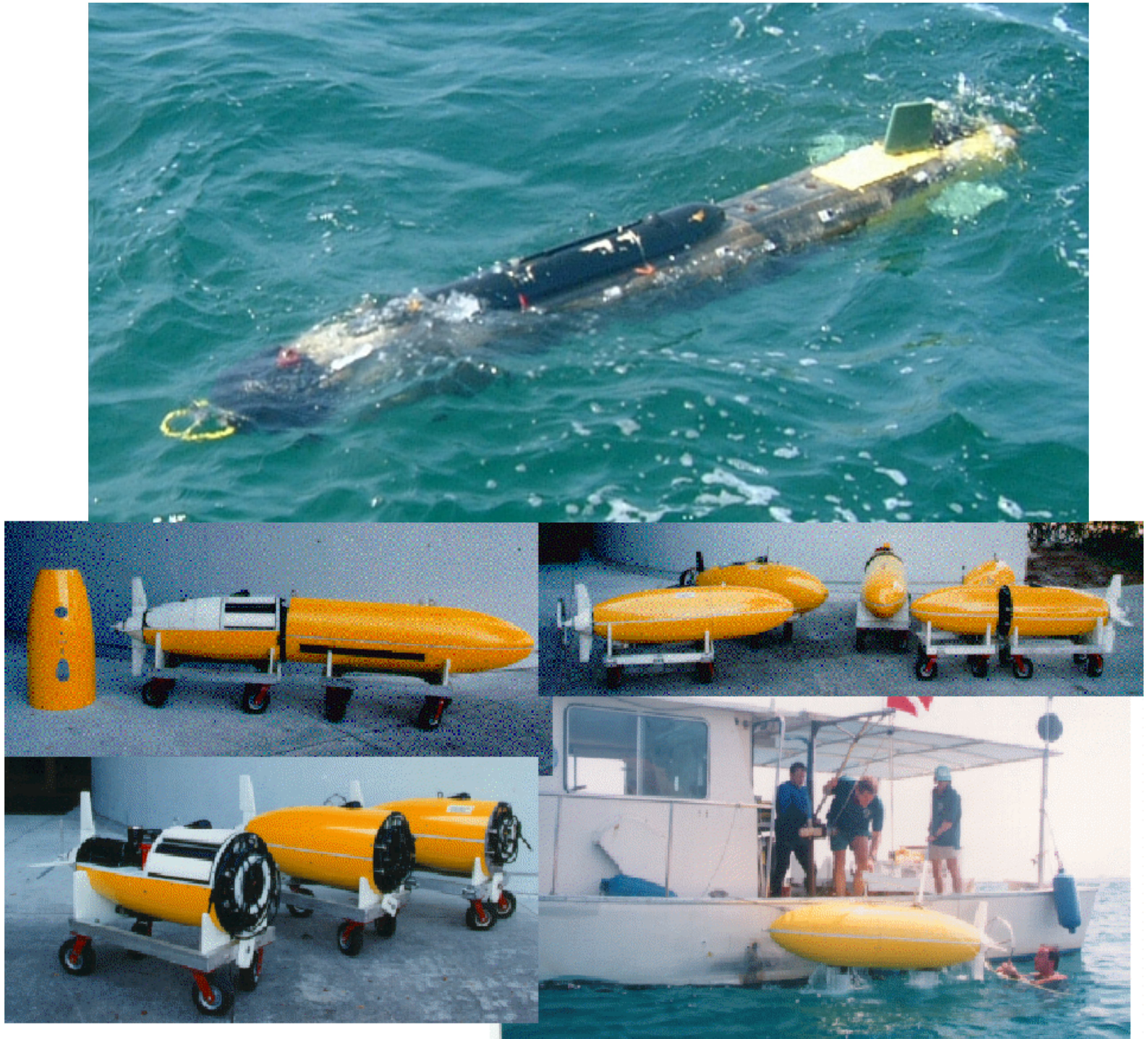
Comprehensive Solutions vs. Incremental Solutions

How to *best* protect citizens from *exploitation*
with citizen-sourced, state-endorsed digital identity

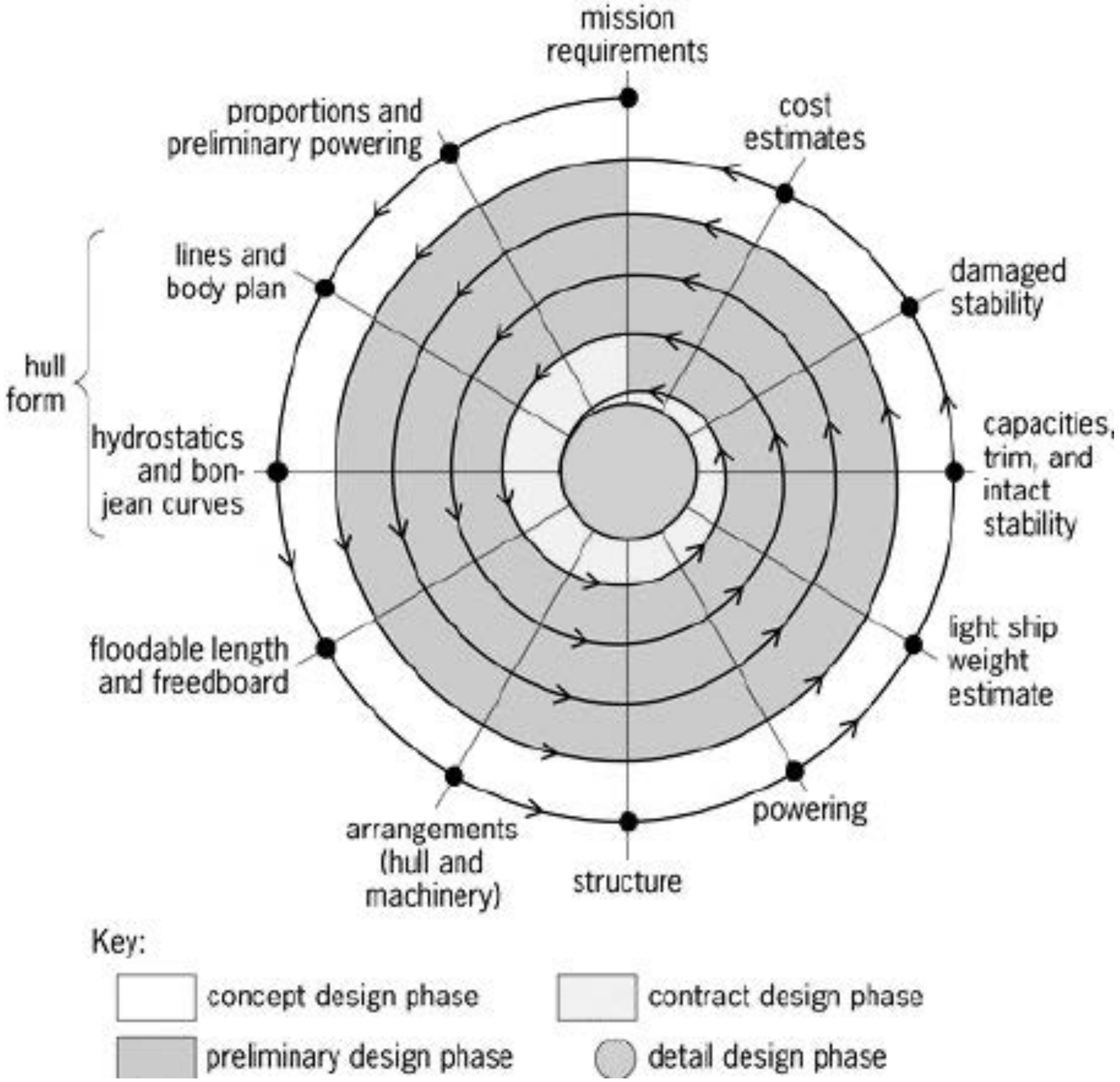
Samuel M. Smith, Ph.D.
sam@kerisuite.org
https://github.com/SmithSamuelM/Papers

2025/10/01

Survivable Systems: AUVs, Ships, Critical Infrastructure



Design Spiral to Explore a Trade Space



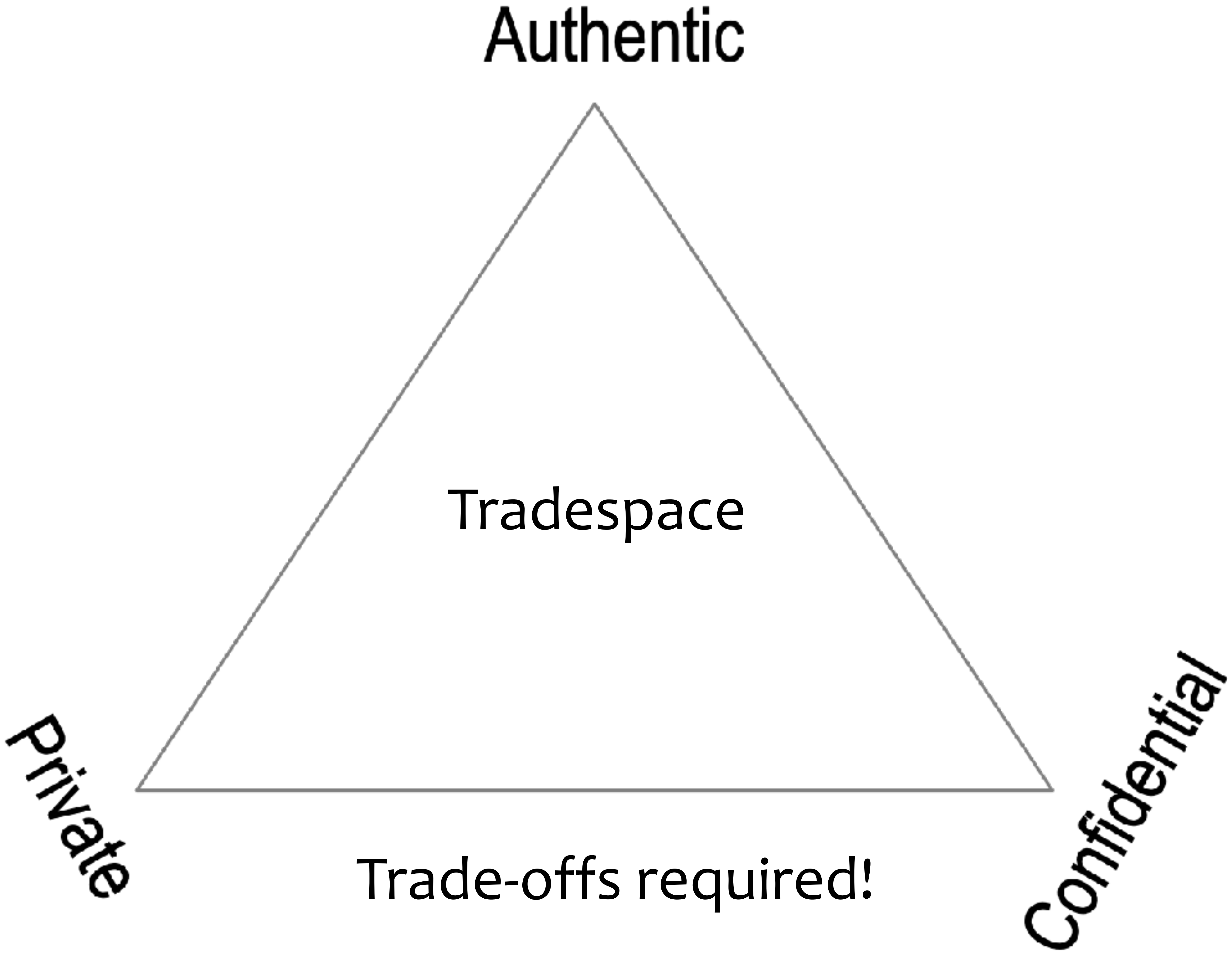
Naval Architecture Design Spiral

https://www.researchgate.net/publication/273026917_Ship_Design_and_System_Integration/figures?lo=1

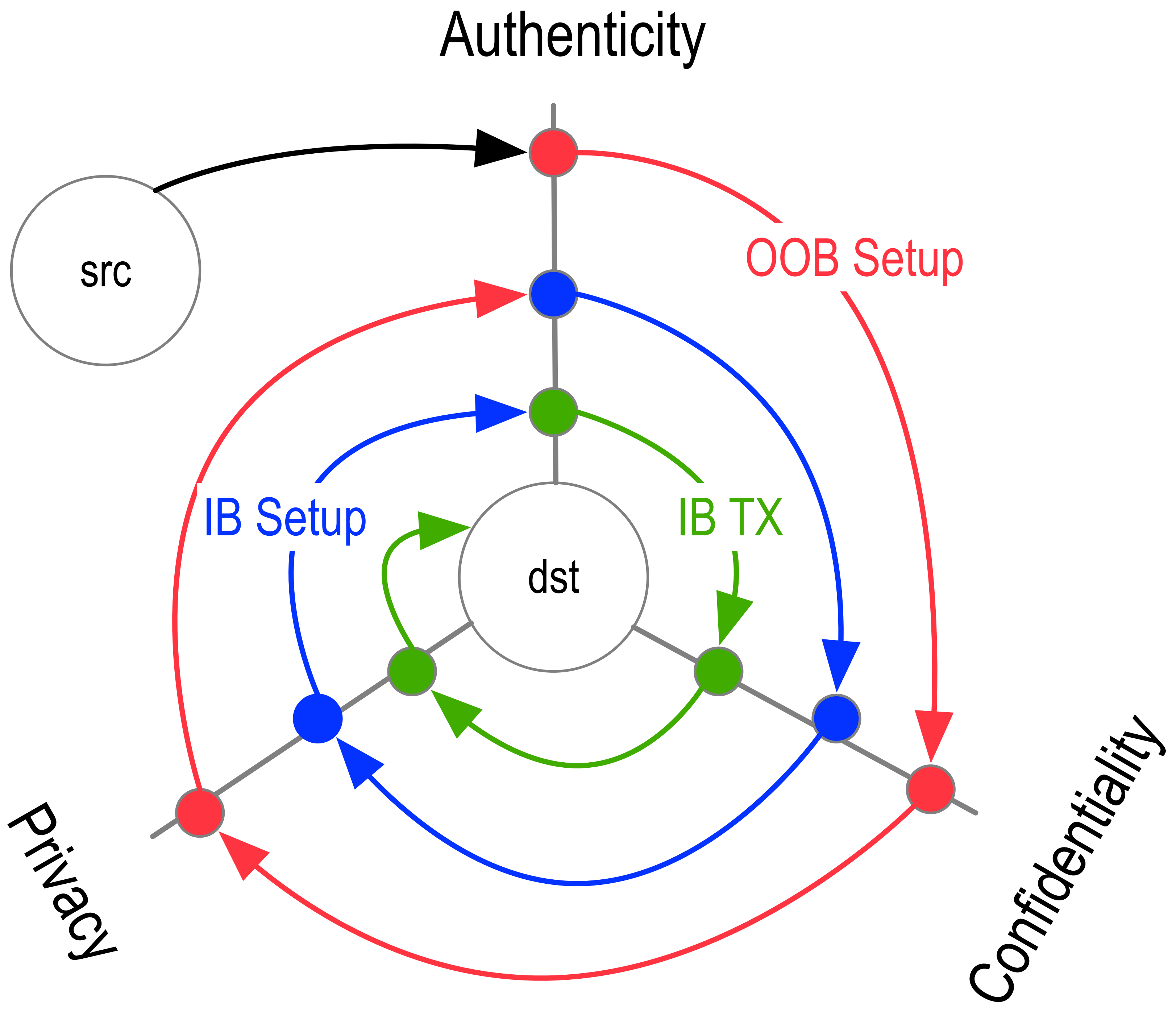
In harsh trade spaces, incorrect a priori decisions often result in highly suboptimal designs.
One must first thoroughly explore the harsh tradeoffs. The PAC trilemma forms a harsh trade space.

PAC Theorem — Trilemma

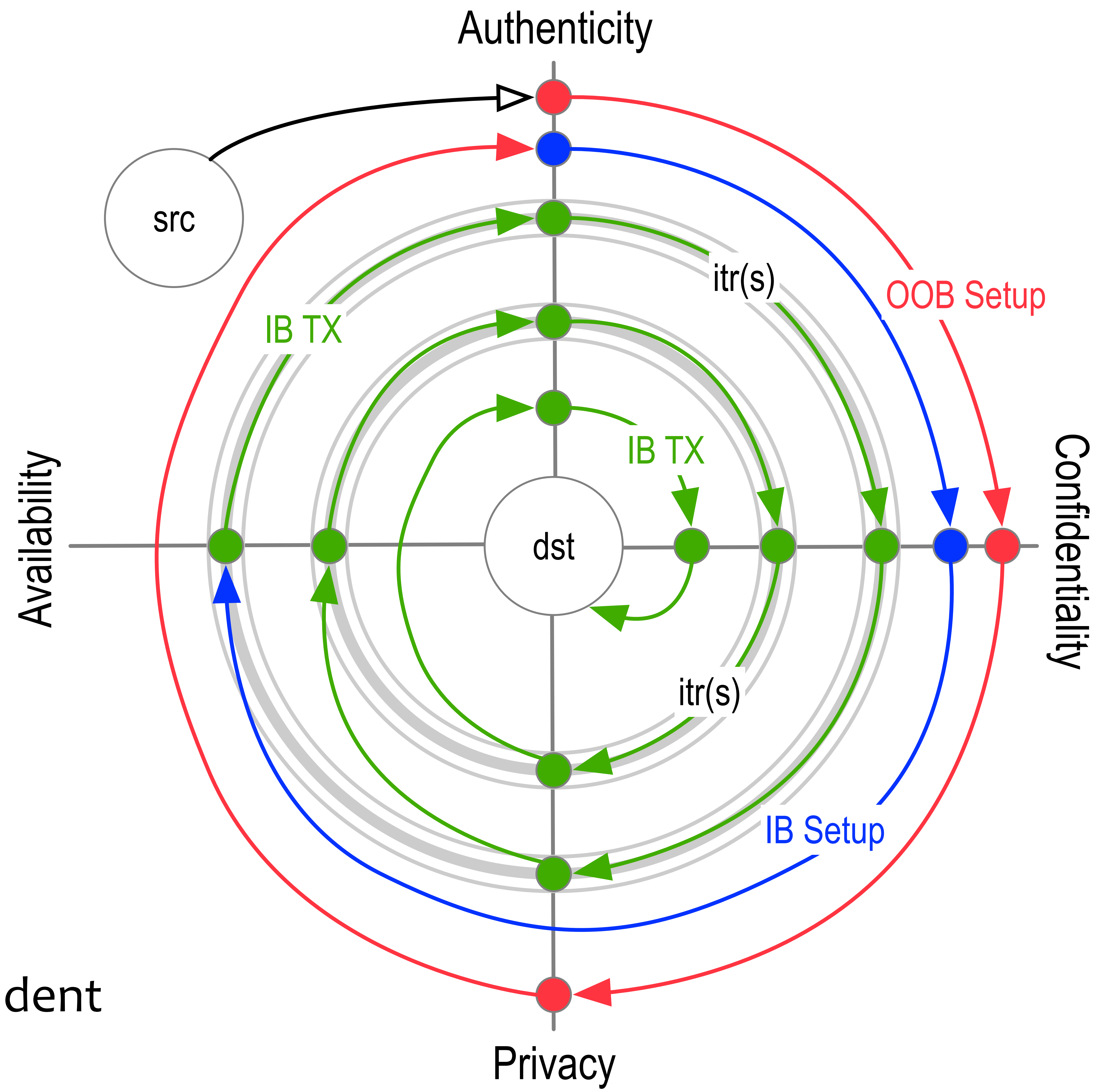
An interaction between two parties may be two of the three, *private*, *authentic*, and *confidential* at the highest degree, but not all three at the highest degree.



Layered Security Overlays



Layered Security Overlay Spiral



Layered Security Overlay Spiral

Setups may be application dependent & hence overlay ordering dependent
Each setup requires one OOBA factor to protect against MITM attack
Setups may be costly, especially those with repeated OOBAs
Interactive setups are not as scalable as non-interactive setups
Trade-offs required

OWASP Top Ten Security Risks

https://owasp.org/www-project-top-ten/

- **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category. (Recursive Privilege Escalation Attacks)
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise. (Key Management, Stale Crypto)
- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures. (Architecture flaws, Trust boundary violations)
- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it’s not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping. (Shared secrets anyone, recursive privilege escalation attacks)
- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
- **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn’t well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it’s not illustrated in the data at this time. (recursive privilege escalation attacks)

OWASP GenAI Security Project https://genai.owasp.org/

Survivable Security

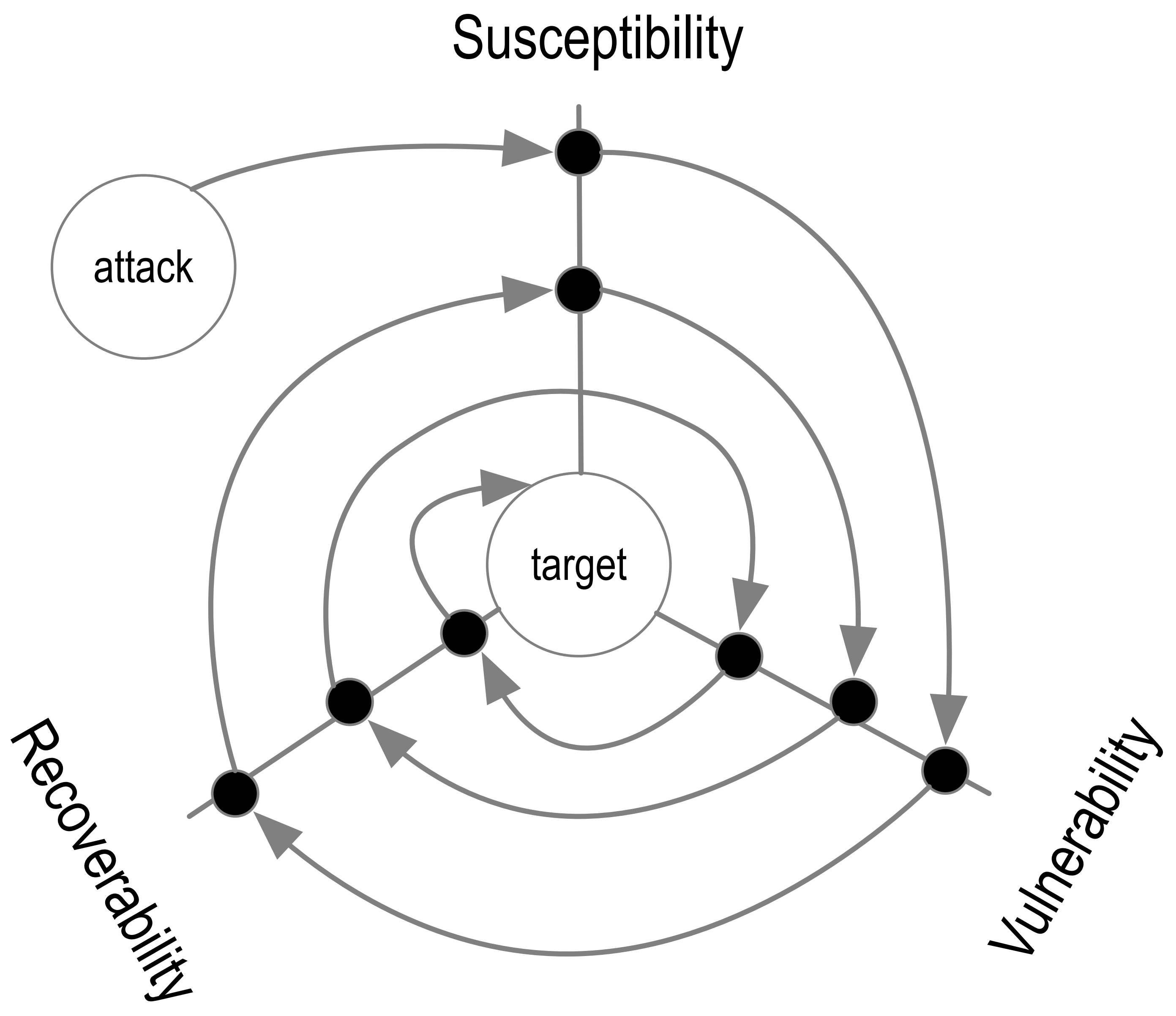
Survivability:

- Susceptibility – Likelihood of being attacked
- Vulnerability – Likelihood of success and extent of harm given an attack
- Recoverability – Likelihood and extent of recovery from a successful attack

A system may be highly vulnerable but not highly susceptible to attack

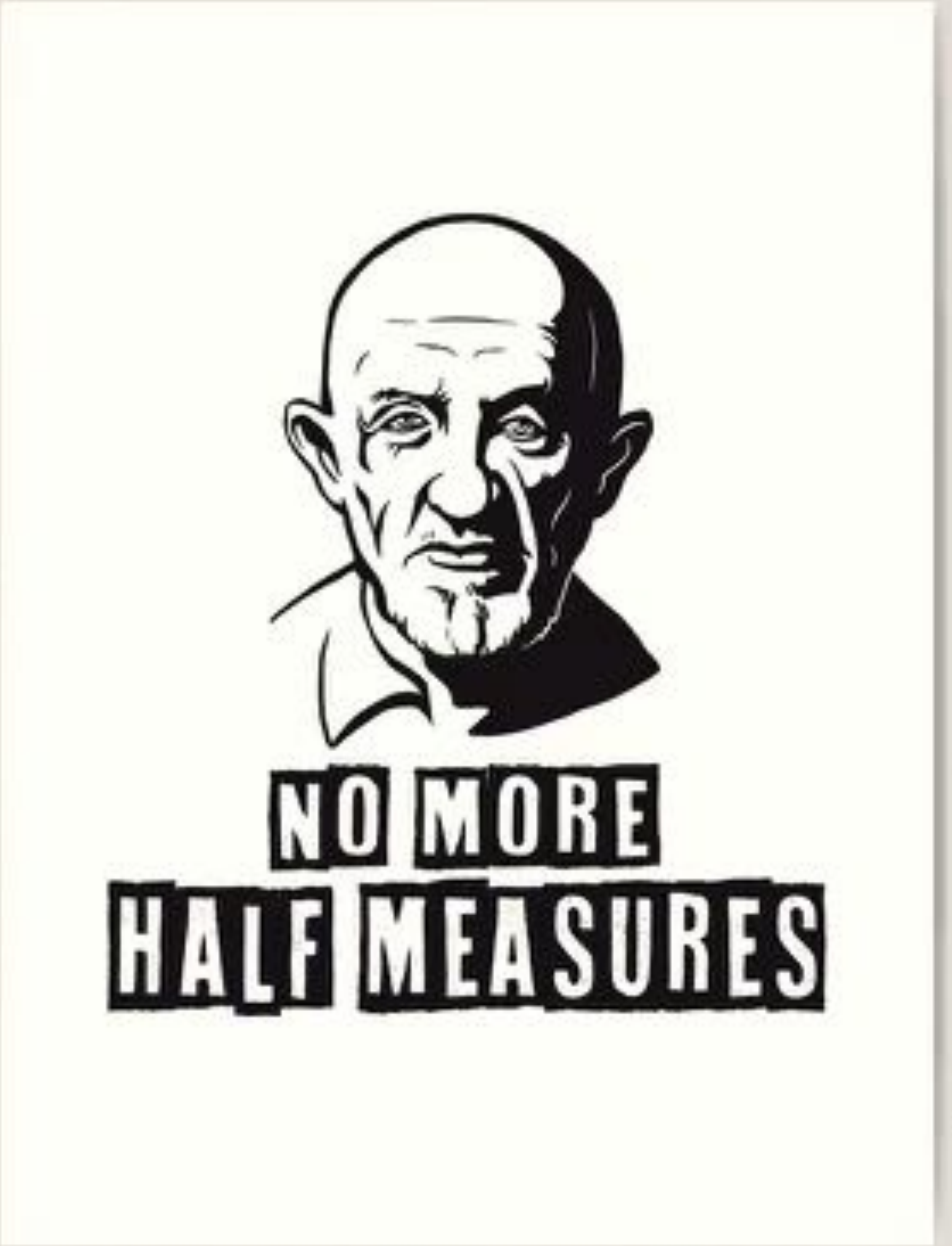
In IT security, susceptibility stems from the return on investment (ROI) of an attack

The “trap” of confusing low susceptibility with low vulnerability



Layered Survivabilty Overlay Spiral

Security First, Always



Minimally Sufficient Means

Adoptable *White Magic* Crypto

Why key compromise is the hard problem for SEDI

Invalid to assume that compromise of the issuer key is impossible.

Key compromise enables verifiable forged issuances (impersonation fraud of the issuer, identity theft of every issuee)

Unanchored forged issuances are not detectable (in general) and therefore preclude specific recovery.

Cannot ensure a timely recovery from forged issuances when those forged issuances are undetectable by the issuer.

Anon (ZKP) signatures are unlinkable to specific forged issuances, and hence, specific forged issuances are undetectable by the issuer.

Cannot ensure a focused recovery of specific forged issuances that are unlinkable and hence undetectable by the issuer.

The risk of forgery persists throughout the lifespan of unanchored long-term issuances, even after the rotation of compromised keys.

Unanchored long-term non-post-quantum-safe signed issuances are vulnerable to the surprise quantum key compromise armageddon

Given unanchored and/or unlinkable issuances, the only way to ensure full recovery from a likely or potential key compromise is to revoke and reissue all issuances made with likely or potentially compromised keys.

Prophylactic key rotation bounds the time frame of potential key compromise by multiplying the frequency and hence cost of revoking and replacing all issuances at each rotation.

Government issuances to millions of citizens exponentially increase the ROI of attackers and, hence, the susceptibility of key compromise.

Revoking and reissuing millions or tens of millions of Government issuances due to likely or potential key compromise is impractical.

As a government, how can you practically recover from a likely or potential key compromise with millions of issuances?

Anchored issuances are linkable and thereby enable the detection of specific forgery and the specific recovery of forged issuances.

Specific recovery is a viable and practical solution to the hard problem of key compromise for SEDI

EUDID Wallet Comparison

Security Considerations of EUDID Wallet: (EUROSmart – EU digital security industry standards White Paper)

"Breaches to the Digital Identity ecosystem have the potential to disclose the identity of all citizens leading to massive frauds and impersonation which would ultimately annihilate any Trust Services operations as a result of broken trust."

https://www.eurosmart.com/wp-content/uploads/2025/04/2025-04-10-Position-paper-on-Security-considerations-for-the-European-Digital-Identity-Wallet.pdf

"The IdP's private keys, which are used to sign assertions, need to be protected from subscribers, RPs, and other unintended parties. If the IdP's private keys are compromised, an attacker could generate arbitrary assertions and impersonate any subscriber on the network at any RP." https://pages.nist.gov/800-63-3-Implementation-Resources/63C/IdP/#:~:text=The IdP's private keys, which,abuse of this key material.

Annex 2- ARF https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/annexes/annex-2/annex-2-high-level-requirements/

A PID Provider or Attestation Provider SHALL revoke a PID or attestation at least:

- upon the explicit request of the User,
- when its security has been compromised,
- upon the death of the User or cease of activity of the legal person who is the subject of the attestation.

Black Magic Crypto is a Security, Policy, and Adoption Risk.

New crypto algorithms need years to prove out their security. Premature adoption risks catastrophic security and/or policy failure. Example BBS+.

"On the Concrete Security of BBS/BBS+ Signatures" 2025/09/27 Proves BBS+ does not satisfy SUF for EUDID. https://eprint.iacr.org/2025/1093.pdf

However, the integration of ZKPs in the EUDI Wallet ecosystem is still under discussion and development due to the complexity of implementing ZKP solutions in secure hardware and the lack of support in currently available secure hardware (WSCDs). https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/

"Current efficient Anonymous Credentials protocols such as CL, PS or BBS/BBS+, do not meet these requirements: they either make use of pairings or pairing-friendly curves and/or are not supported by current certified secure elements." https://csrc.nist.gov/csrc/media/presentations/2024/wpec2024-3b3/images-media/wpec2024-3b3-slides-antoine-jacques--BBS-sharp-eIDAS2.pdf

BBS# is too new. "Making BBS Anonymous Credentials eIDAS 2.0 Compliant" 2025/04/11 https://eprint.iacr.org/2025/619

There is no viable "today" solution that provides both security and issuer unlinkability.

KERI’s Paradigm Shift: Security First

All ID Privacy Systems (including EUDID), except KERI/ACDC, assume that “unlinkability” is an end in and of itself.

Yet, these same systems include exceptions, such as payments, where linkability is necessary to prevent fraud.

This exposes a flaw in the assumption that unlinkability is, in fact, the desired goal.

Therefore, the axiomatic assumption that the goal is privacy first, as unlinkability, cannot be true.

KERI/ACDC postulates that the end goal is not unlinkability, but rather unexploitability through the strongest security.

Because there are no significant exceptions to this goal, the axiomatic assumption that unexploitability is indeed the goal is likely true.

Unexploitable vs Unlinkable

Decorrelation vs Deidentification

Accountability vs Anonymity

Shift from fixing leaks to fixing exploitation!

Strongly incentivize decorrelation instead of “wack-a-mole” attempts at removing all points of correlation.

Decorrelation comes from inverting the economics of correlation.

Exploitation protection comes from comprehensive retroactive anti-assimilation incentives

Impossible Goal

Eliminate impersonation fraud, of me, to me, and by me: (no more identity theft because the ROI is negative).

What is the value of achieving this goal?

- To citizens?
- To private industry?
- To governments?

What exploitation of citizens using their digital identity remains once identity theft is eliminated?

- Tracking?
- Exploitation by whom? Rate and rank harm by who does the tracking
  - Government?
    - Foreign?
    - Federal?
    - State?
    - Local?
  - Private Industry?
    - Attention theft?
  - Hackers?

What is the net benefit of fraud-free vs. non-fraud-free ecosystems?

KERI/ACDC Security Properties

All exploits must begin with the compromise of (asymmetric) private signing keys

Any exploit that compromises private key(s) must be nearly instantaneously detectable

Detected private key compromise must be automatically recoverable using quantum-safe one-time-use pre-rotated keys

Controller Key state may be made highly available via its own witness pool

Private key compromise and hence exploitation may be made exponentially more difficult through a combination of three threshold structures: multi-signature, MFA witness pools, and delegated identifiers

Validators are protected from dead (stale) key compromise via the first-seen policy enforced by their own watcher network

Validators are protected from live key compromise via duplicity evident property with respect to the controller's key state

Reconciliation policies must enable exploited controllers to recover from a live key compromise

Validators may be protected from malicious eclipse attacks on key state via the duplicity-evident watcher network

Issuances (Entitlements or AuthZ) are similarly protected by anchoring to the key state

Unbounded term issuances are verifiable despite key rotation when anchored to the key state

High-stakes issuances may gain extra protection by interleaving anchoring with waiting periods that force in-stride detectability and blockage of live exploit attempts.

Everything must be provable via verifiable data structures, no trusted third parties, no shared secrets, no platform lock-in

Infrastructure must be highly portable, with no shared governance between the controller's witness network and the validator's watcher network. Similarly, between the Issuer's registrar and the validator's observer.

Unique features of KERI/ACDC that require Issuer linkability

Near-instantaneous detection key compromise given an impersonation fraud attack

Near-instantaneous recovery from key compromise and defeat of impersonation fraud attack

= no external attacker impersonation fraud.

Global detectability of duplicity by malicious Issuers due to Watcher Network

= no malicious Issuer impersonation fraud

Delegated identifiers = vertical and horizontal scaling of signing infrastructure

Multi-threshold protection from key compromise attack

- Multi-signature AIDs
- MFA witness pools
- Delegated identifier chains

Secure practical, dynamically revocable delegated chains of authority (ACDCs) that persist across key rotations

= secure guardianship

= secure organizational identity

= secure authorization chains

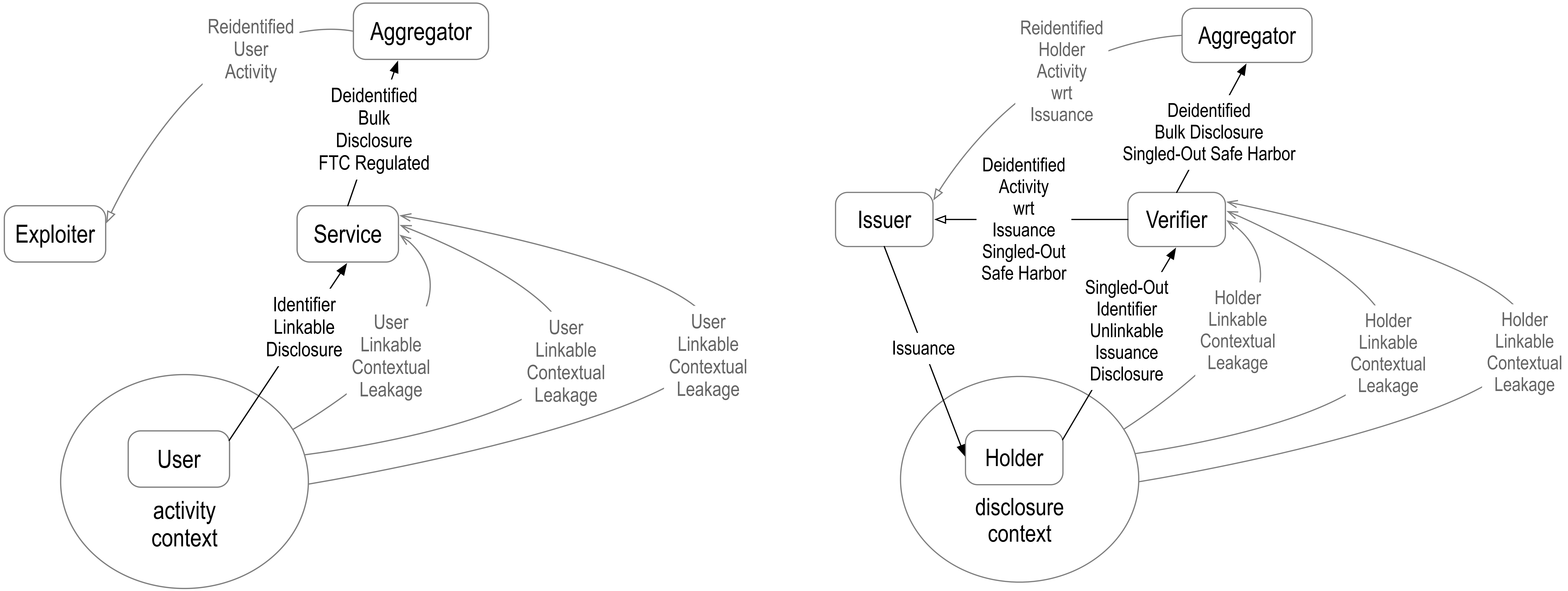
Highly available citizen-sourced identities via citizen witness pools

Verifiable reputation via ACDC chained evidence dossiers

Multiple roots-of-trust for reputation

Strongest Identity assurance amortized over the lifespan of unbounded term (persistence) AIDs

Where we are


Reidentified User Activity
Aggregator
Deidentified Bulk Disclosure FTC Regulated
Exploiter
Service
Identifier Linkable Disclosure
User Linkable Contextual Leakage
User Linkable Contextual Leakage
User Linkable Contextual Leakage
User
activity context
Reidentified Holder Activity wrt Issuance
Aggregator
Deidentified Bulk Disclosure Singled-Out Safe Harbor
Issuer
Deidentified Activity wrt Issuance Singled-Out Safe Harbor
Verifier
Singled-Out Identifier Unlinkable Issuance Disclosure
Holder Linkable Contextual Leakage
Holder Linkable Contextual Leakage
Holder Linkable Contextual Leakage
Issuance
Holder
disclosure context

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 B 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 B Records: https://npdbreach.com/

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

Health Care Data Breaches: 2024 276 M+ , 2023 168 M+ Cumulative 2009-present : 846 M+ records: https://www.hipaajournal.com/healthcare-data-breach-statistics/

MS Sharepoint Breach ZeroDay 400 Servers: https://www.hornetsecurity.com/en/blog/sharepoint-vulnerability/

Google 2.5 B Users 2025/08/26: https://news.trendmicro.com/2025/08/26/google-data-breach-gmail/

Reach and Scope of Modern Data Aggregators:

- Probability Waterfall https://transmitsecurity.com/blog/private-browsing-mode-detection-and-its-potential-fraudulent-use-cases
- POT Data Brokers, global coverage, multi-constellation << $0.01 per point: Bloomberg https://secondmeasure.com/

ChatGPT4 = 1 PetaByte Training Data Set Size

Generative Agentic AK connected services

Nation State Funded 5GW (Fifth Generation Warfare)

Design for the Future of Correlatability not the Past

What is not easily and cheaply correlatable today will be exponentially easier and cheaper to correlate in 2 years, 5 years, 10 years.

Generative Agentic AI-connected data broker services will enable anyone to surveil anyone else anywhere, with natural language queries for pennies per target.

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.

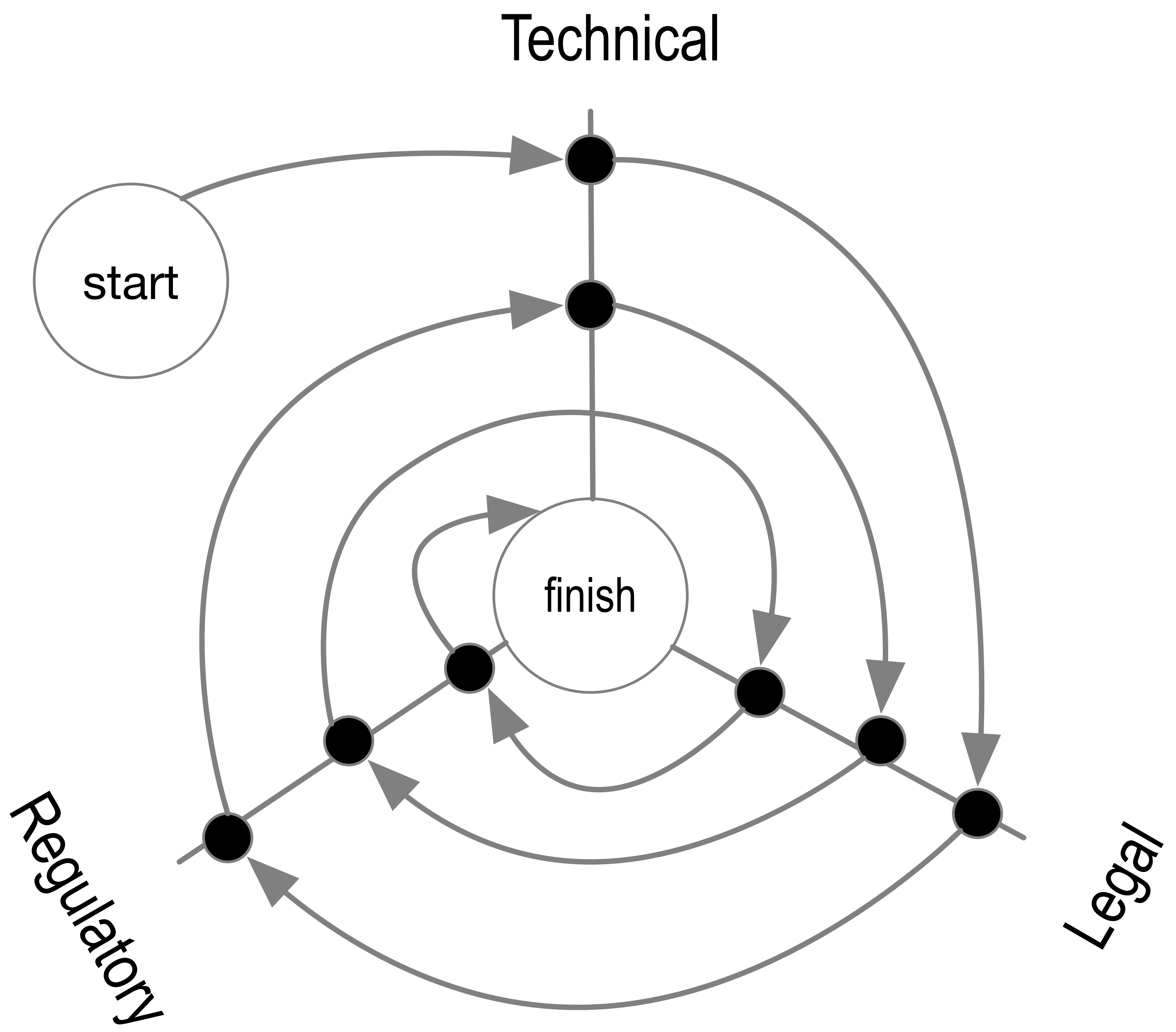
The only individuals for whom this is not true are those that are “off-grid” or have fake identities

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?

Comprehensive Decorrelation Incentivization



Layered Decorrelation Incentives Spiral

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 ultimately matters is full "contextual unlinkability,"

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

Therefore, providing unqualified "unlinkability" is not a viable policy goal.

The false attraction of unlinkability

The concept of unlinkability is attractive primarily because it purports to provide a largely technological solution to what is otherwise a complex and so far intractable problem involving economic, legal, regulatory, and social issues.

It is trying to cure the symptom of the disease, not the disease itself.

True unlinkability requires eliminating all "points-of-correlation", which is impossible.

Unlinkability is a "*wack-a-mole*" approach to privacy, incremental vs. comprehensive.

If one does not first employ economic, legal, regulatory, and social solutions to privacy, then merely pursuing unlinkability is "privacy theater".

Indeed, authentic points of correlation may be essential to enable counter-incentives to exploitation.

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.
- Undetected key compromise enables impersonation of the Issuer thereby incentivizing Issuer employees to exfiltrate private keys.
- Thus the ***security dilemma*** of cryptographic unlinkability: given Issuer key compromise, recovery requires revoking and reissuing all the Issuances used by those keys because there is no way to "link" a given issuance past or future to a compromised vs uncompromised use of those keys (without breaking unlinkability).
- Impractical for any long term issuances such as birth certificate SEDI etc
- 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 such as chain-link-confidentialty. A enforceable confidential contract requires 1) an agreement, 2) an exchange of consideration, and 3) an intention to create legal relations. #3 is defeated by unlinkability.

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 (Data Loyalty) 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/metadata, requires a mixture of legal, regulatory, economic, and technical mechanisms.
- *Cryptographic unlinkability defeats legal, contractual, and economic accountability, which are essential to solve the hard problem of contextual leakage!*

Unlinkable ≠ Untrackable

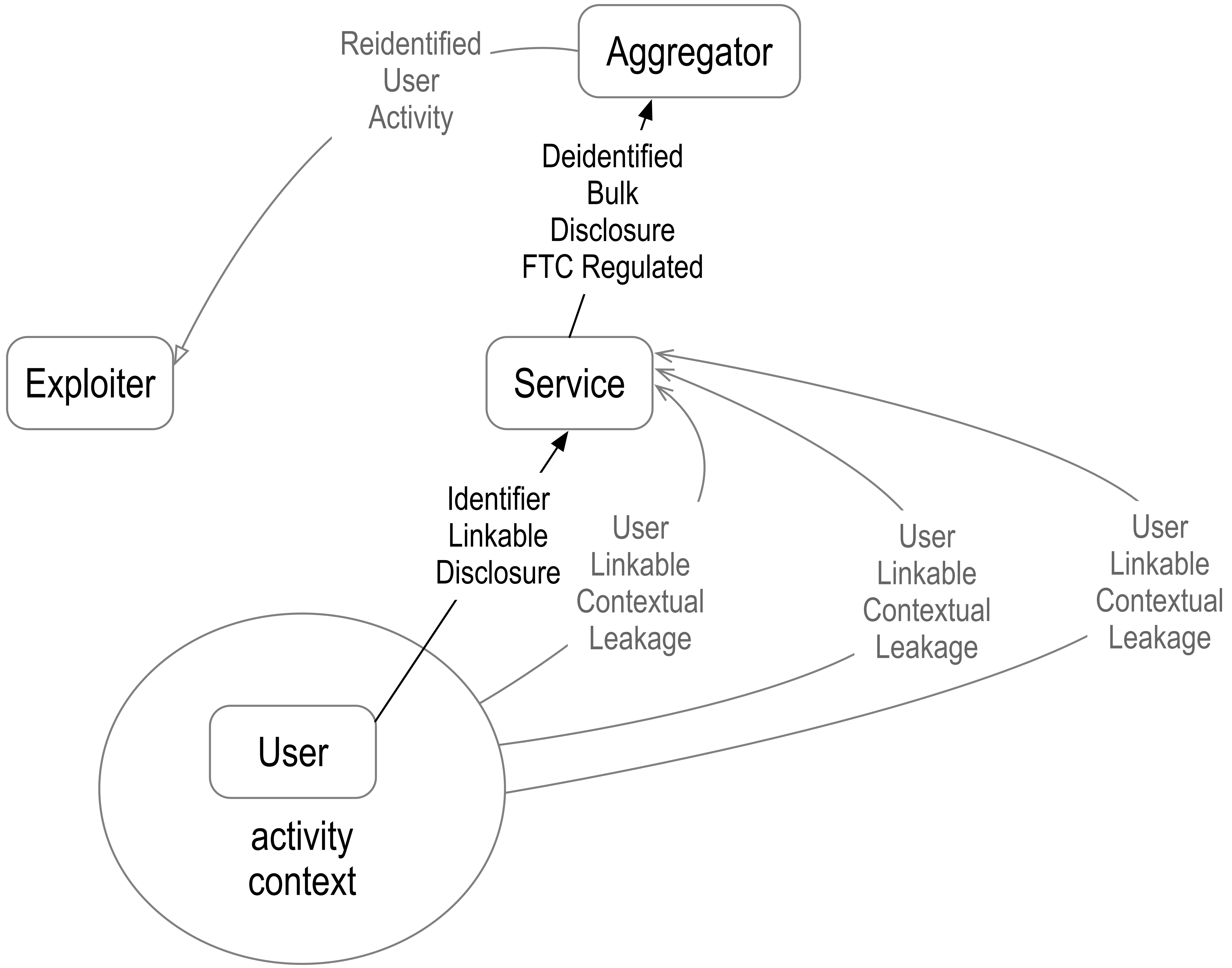
Cryptographic unlinkability, as applied to disclosed data, means the data is pre-deidentified.

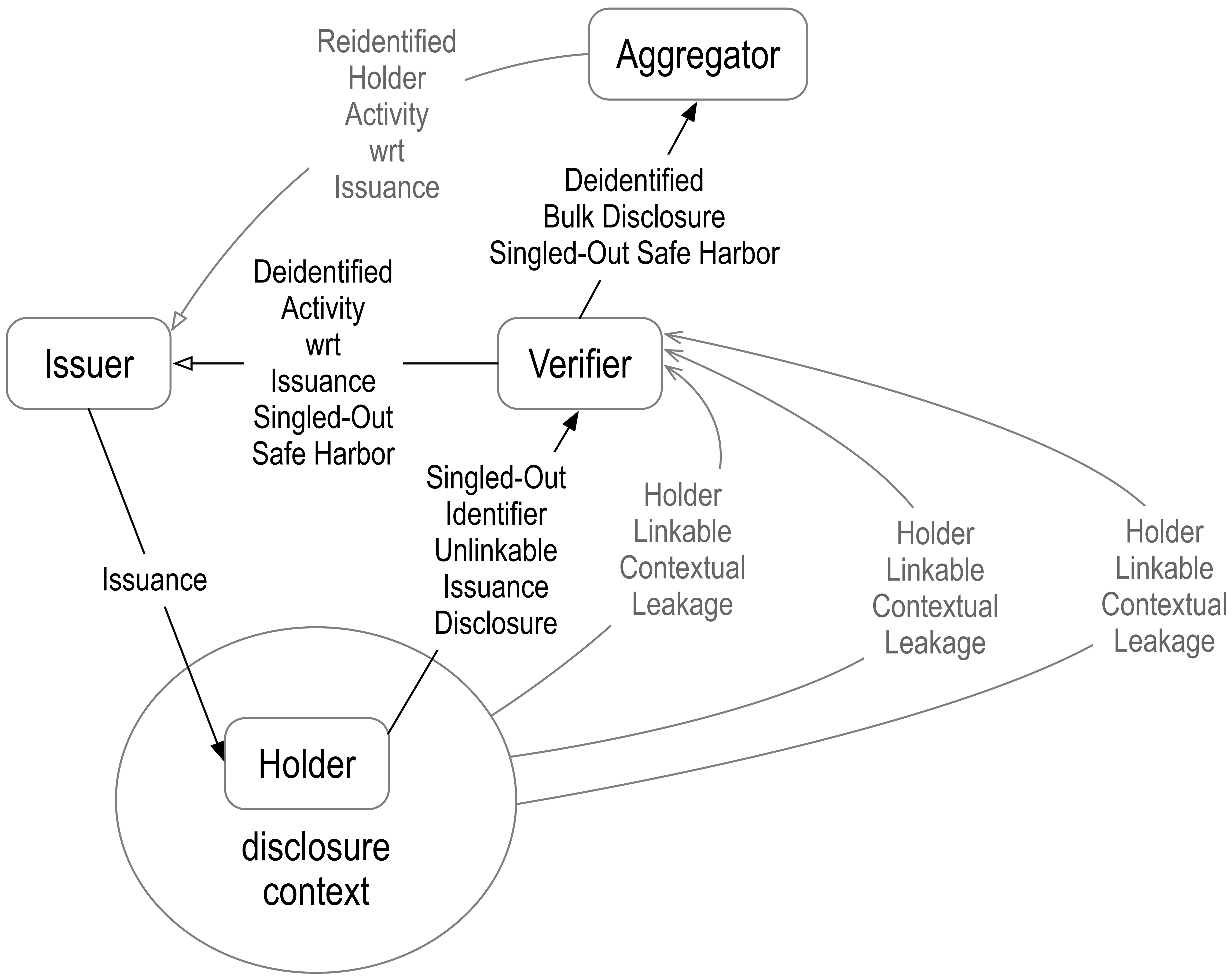
The economics of super correlators (data brokers, super aggregators, generative AIs) have resulted in tooling that enables them to track despite unlinkable (deidentified) data.

By default, they assume the data they collect is already deidentified (i.e., is unlinkable).

Unlinkability of data makes no material difference in how a super correlator operates.

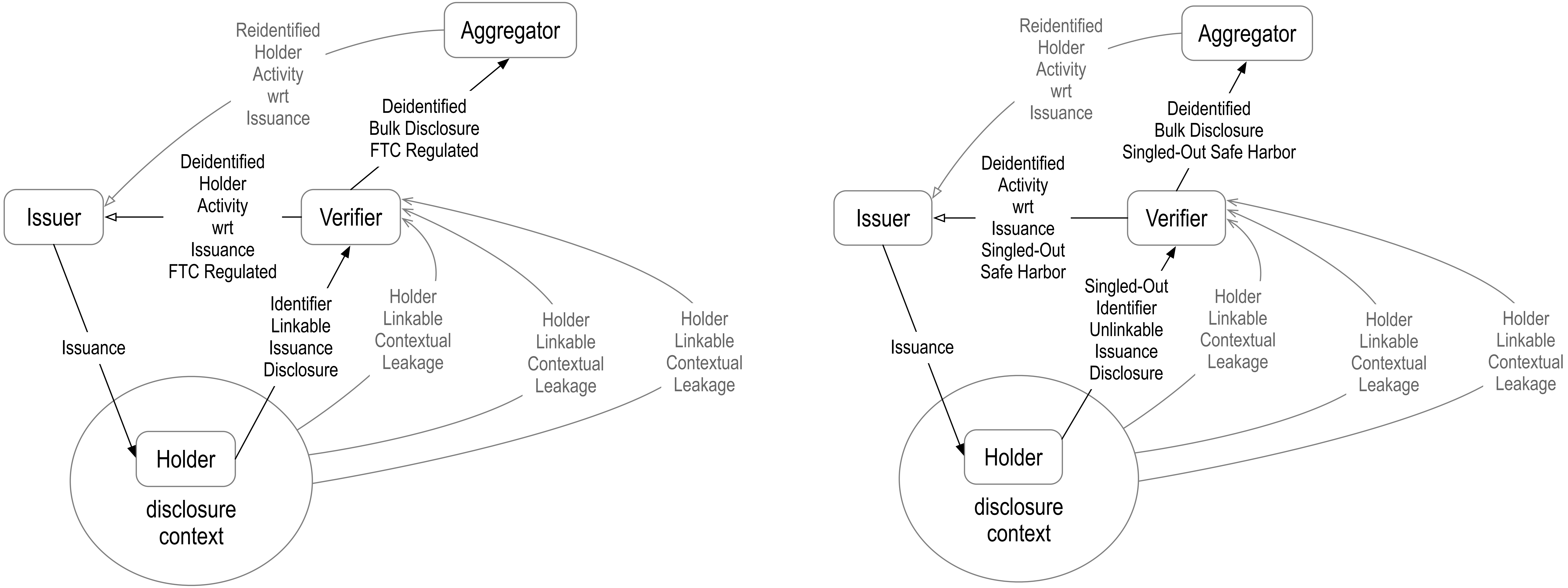
contextual linkability reidentification





special case of de-identified, re-identification but made easier by singling out and regulatory safe harbour

contextual linkability reidentification wrt issuances



An "identifier unlinkable" singled-out act of disclosure does not materially protect the Holder. The ZKP proof required for such a disclosure enables undetectable impersonation attacks on the Issuer and the Holder. Greater harm to Issuers, Verifiers, and Holders.

Hot Wars and Cold Wars

Authenticity and hence confidentiality with KERI/ACDC/TSP is a cold war = no casualties.

Authenticity and confidentiality with PKI/OIDC is a hot war = casualties.

Privacy is always a hot war = casualties.

Hot wars involve rapidly evolving tactics and tech, a resource-constrained war of attrition against potentially vastly superior opponents.

Unlinkability vs Unexploitable (impersonation fraud, identity theft).

A privacy-first approach may result in a potential decrease in hard costs from reducing the privacy attack surface, but it yields a net increase in actual harm due to fraud, breaches, safe-harbor incentives, and lost value capture opportunities relative to a security-first approach.

A security-first approach makes a better risk-mitigation trade-off between exploitable harm and protection cost.

Three Party Information Sharing and Leakage Model

Information is Shared between two parties.

Third party observers may obtain information:

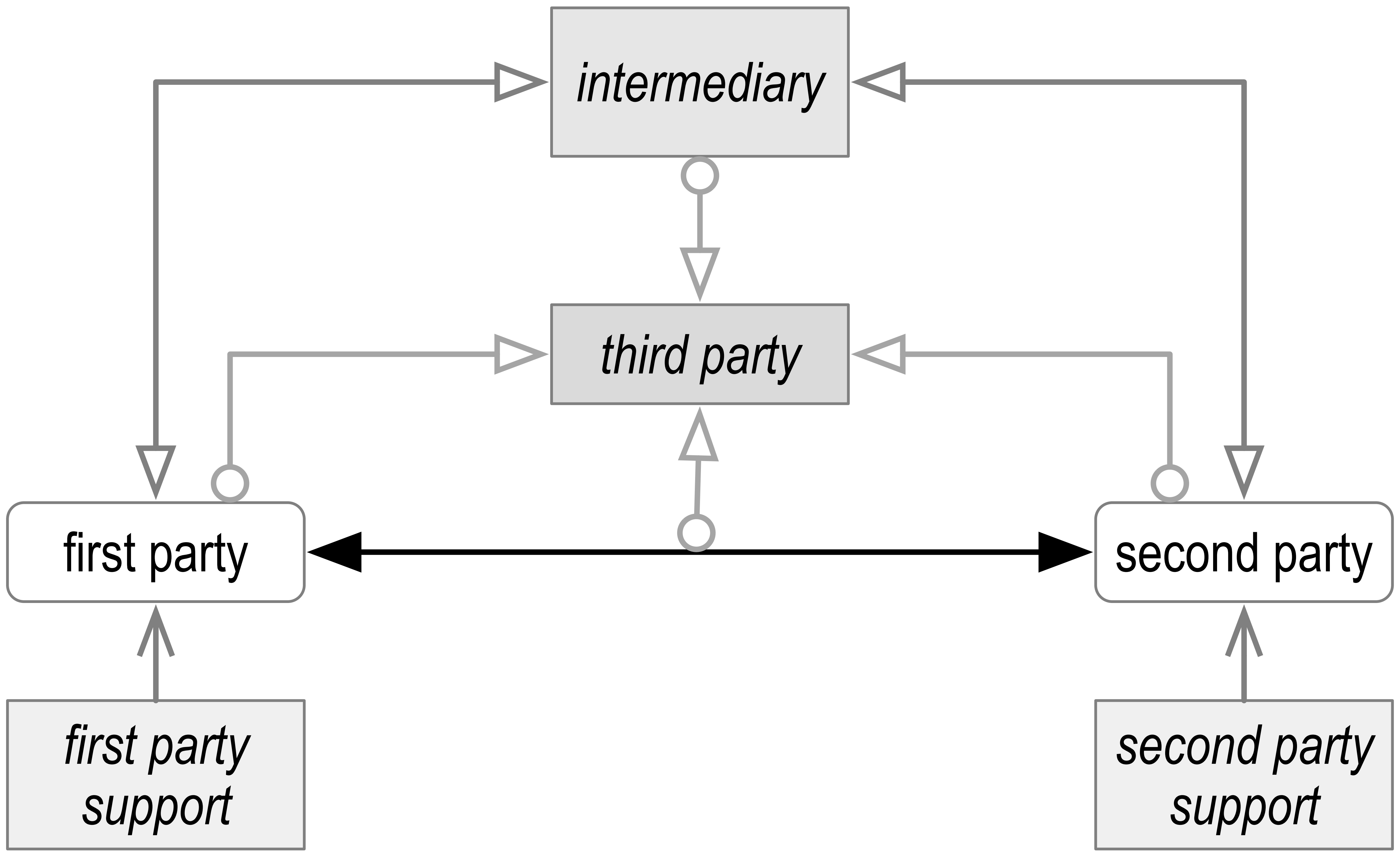
Indirectly as meta-data about the sharing interaction via leakage of the channel.

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.



3rd Party Surveillance

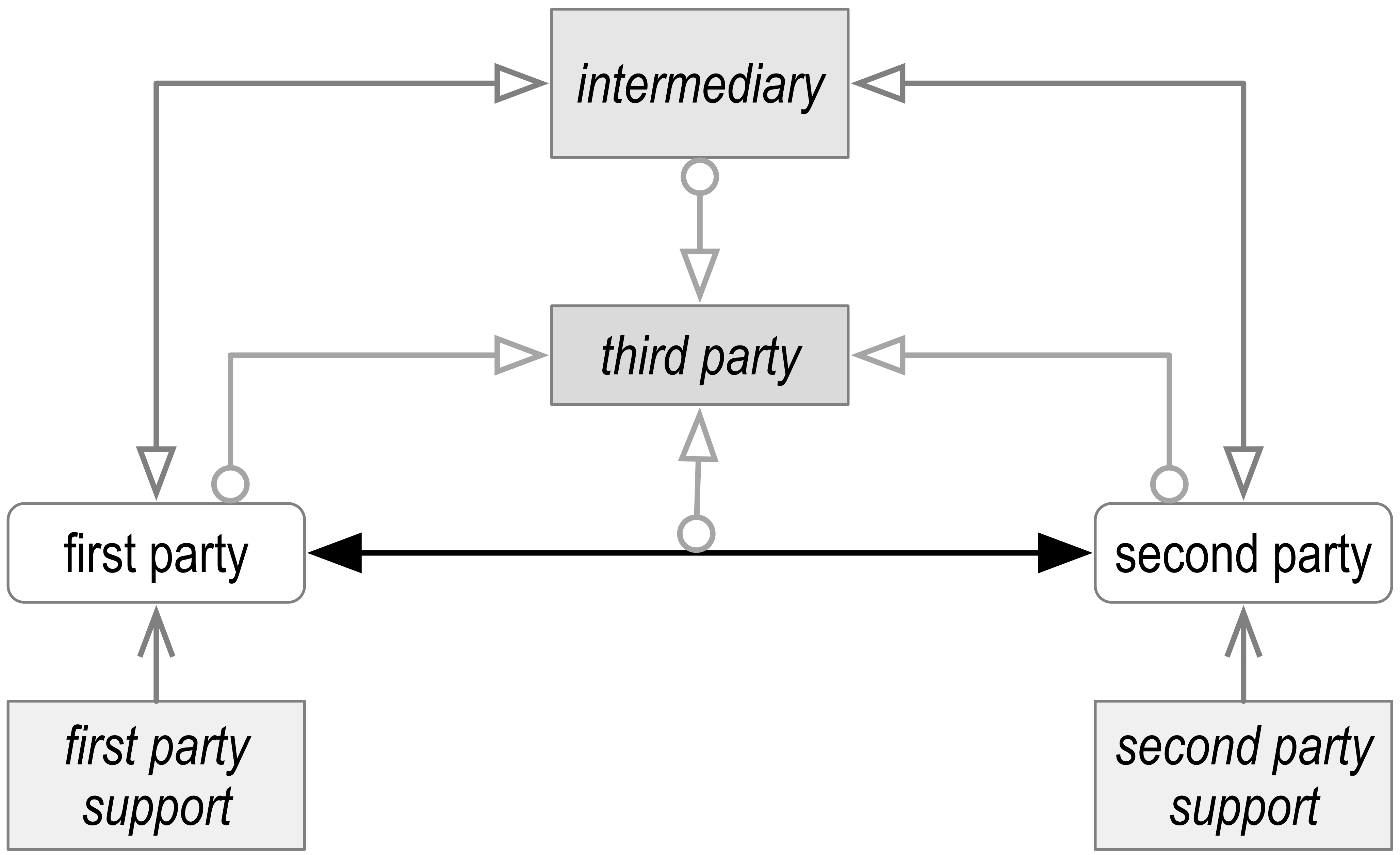
Privacy with respect to the 3rd party is protected if the 3rd party has no knowledge of the identifiers used by the 1st and 2nd parties for the conversation (disclosure).

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.



Three Party Exploitation Model

The 1st and 2nd parties have knowledge of each other via their identifiers. The identifiers are non-content metadata.

The 1st party, as the discloser, has knowledge of the data to be disclosed.

The 1st party discloses data to a 2nd party. The disclosed data is content data.

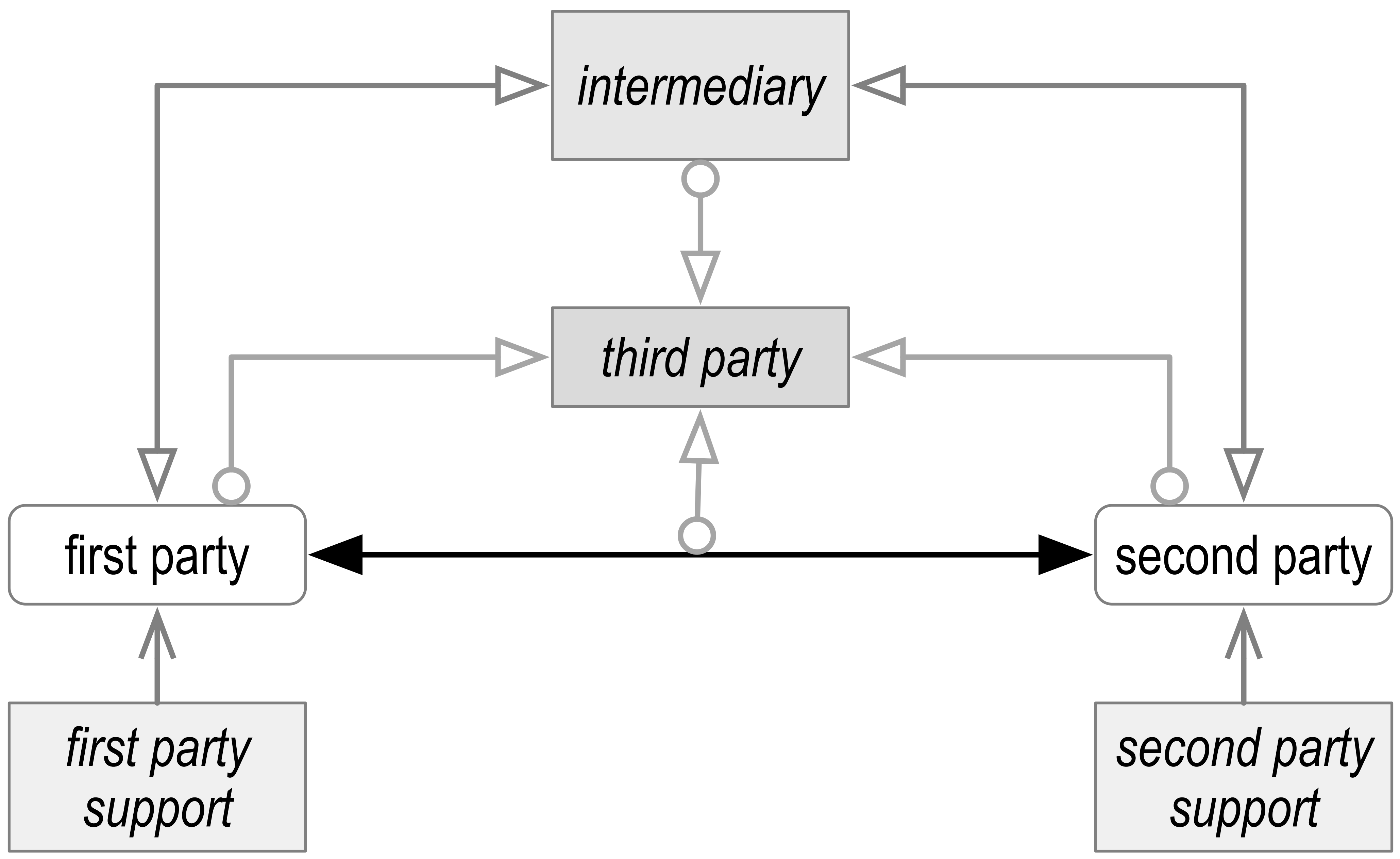
As a result of the disclosure, the 2nd party, as the disclosee, now has knowledge of the disclosed data.

A 2nd party exploits the 1st party by using the disclosed data in any manner that takes advantage of the 1st party.

A 3rd party is any party that is neither a 1st nor 2nd party.

Any use of metadata or content data by the 3rd party can be considered exploitative since it is not permissible.

An intermediary may be considered a 1st, 2nd, or 3rd party depending on how and by whom it is trusted or not.



ACDC Confidentiality/Privacy Protections

Least Disclosure:

- *The system should disclose only the minimum amount of information about a given party needed to facilitate a transaction, and no more*

Graduated Disclosure: progressive least disclosures that each enable further disclosure

- Compact Disclosure
- Metadata Disclosure
- Partial Disclosure
- Nested Partial Disclosure
- Full Disclosure
- Selective Disclosure
- Bulk-issued Instance Disclosure (various degrees of validator-to-validator cryptographic unlinkability)
- Combinations of the above

Contractually Protected Disclosure:

- Uses graduated disclosure to minimize leakage prior to legally enforceable protection
- Chain-Link Confidential Disclosure: strings attached downstream of disclosure, ubiquitous counter-incentive to correlate
- Contingent Disclosure:
  - Conditions for additional disclosure on disclosee, Escrow disclosure, JIT-NTK disclosure, and Latent Accountability
- Legal protection may include retroactive anti-assimilation terms that plug leaks in the graduated disclosure process

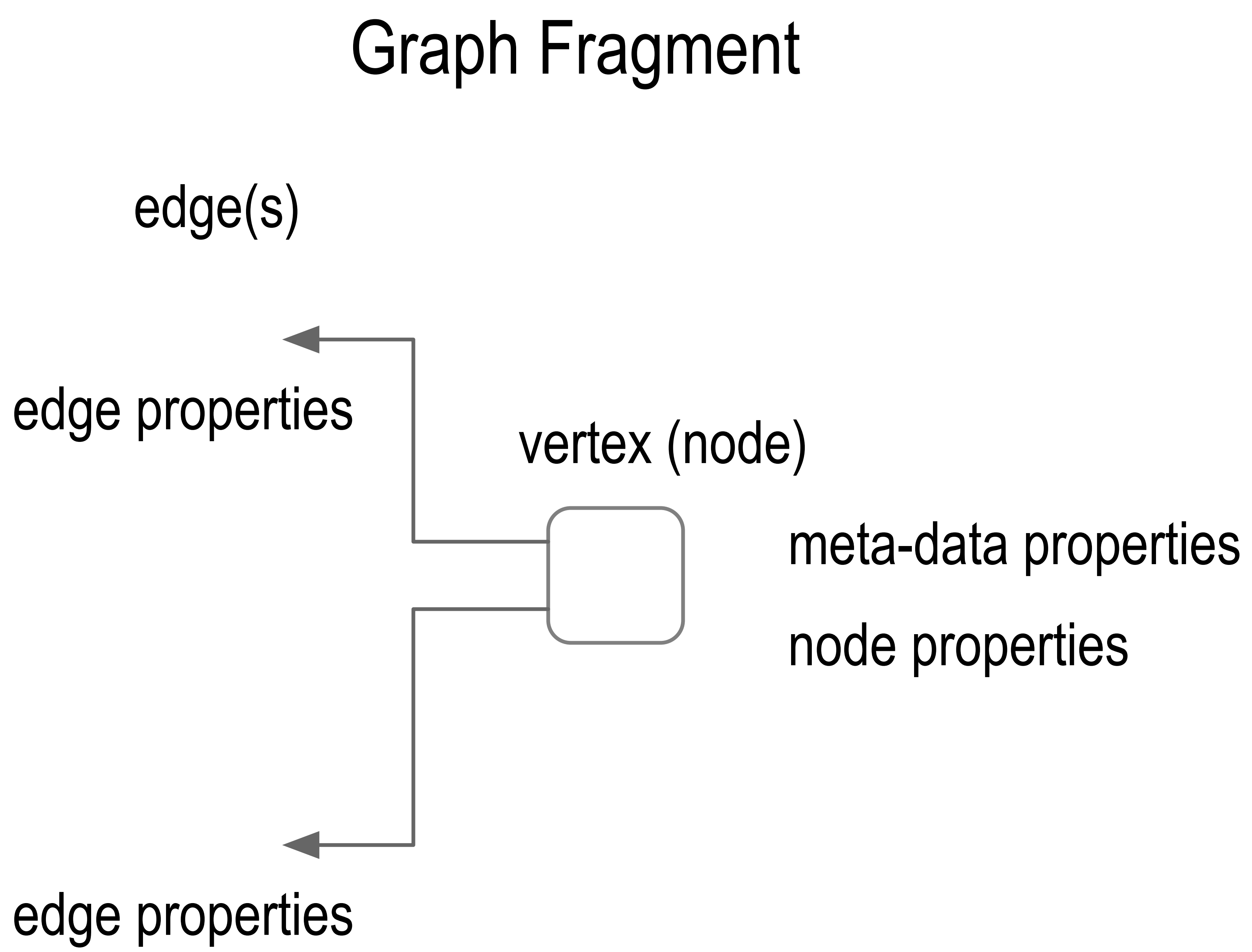
Blindable ACDC State Registries

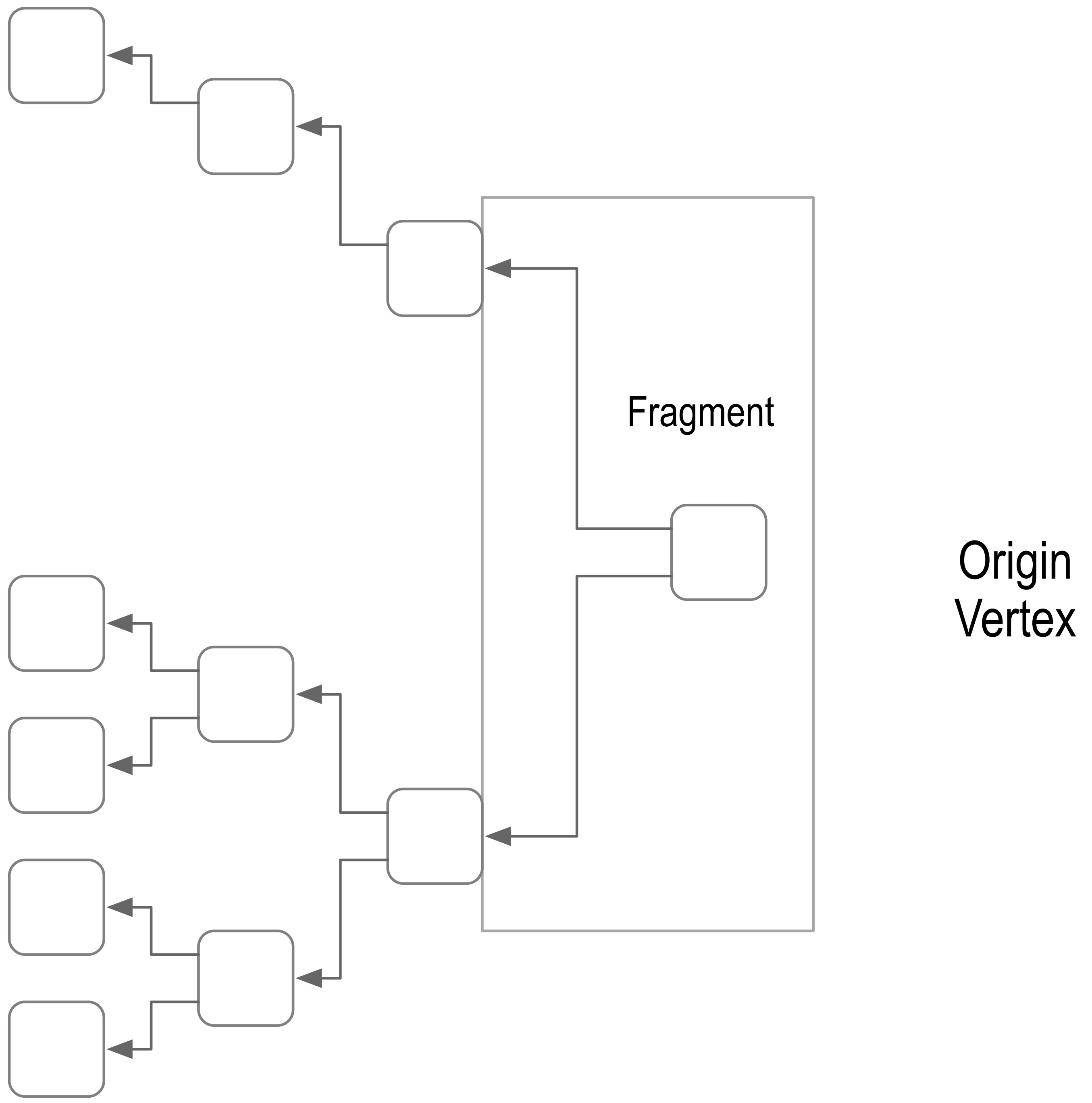
Bindable Blindable Delegated ACDC State Registries (verifiable, persistent, dynamically revocable, chained AuthZ)

IPEX Protocol (issuance and presentation exchange)

Big Picture: What is an ACDC?

- A decentralized, distributed, verifiable data structure that is structurally constrained by an immutable but composable JSON Schema.
- Each ACDC is universally uniquely referenced by its SAID.
- An authenticatable (multiple authors) distributed graph fragment that may be communicated securely.
- Graph fragments use SAIDs to hash-chain themselves together without any expansion needed.
- The composition of graph fragments is an authenticatable, verifiable graph data structure, i.e., a chained set of ACDCs (zero-trust end-verifiable security model)
- Verifiable data structures all the way down





ACDC is a Graduated Disclosable Hash Tree

The different variants of an ACDC form a hash tree (using SAIDs) that is analogous to a Merkle Tree in that the root hash provides an *integrity proof* of the tree.

Signing the top-level SAID of the compact version of the ACDC is equivalent to signing the root hash.

Different variants of an ACDC (SADs with SAIDs) correspond to different branches of the hash tree.

The process of verifying that a section's SAD via its SAID is included in the top-level SAID is a type of *inclusion proof*.

Schema as type: The schema SAID is a universally unique type identifier for the ACDC.

Composable sub-schemata enable graduated disclosable variants to share the same SAID as the type.

The most compact SAID computation enables all graduated variants to share the same ACDC SAID.

A single anchor of the ACDC SAID provides *proof of issuance* of any graduated disclosable variant of an ACDC at the time of presentation.

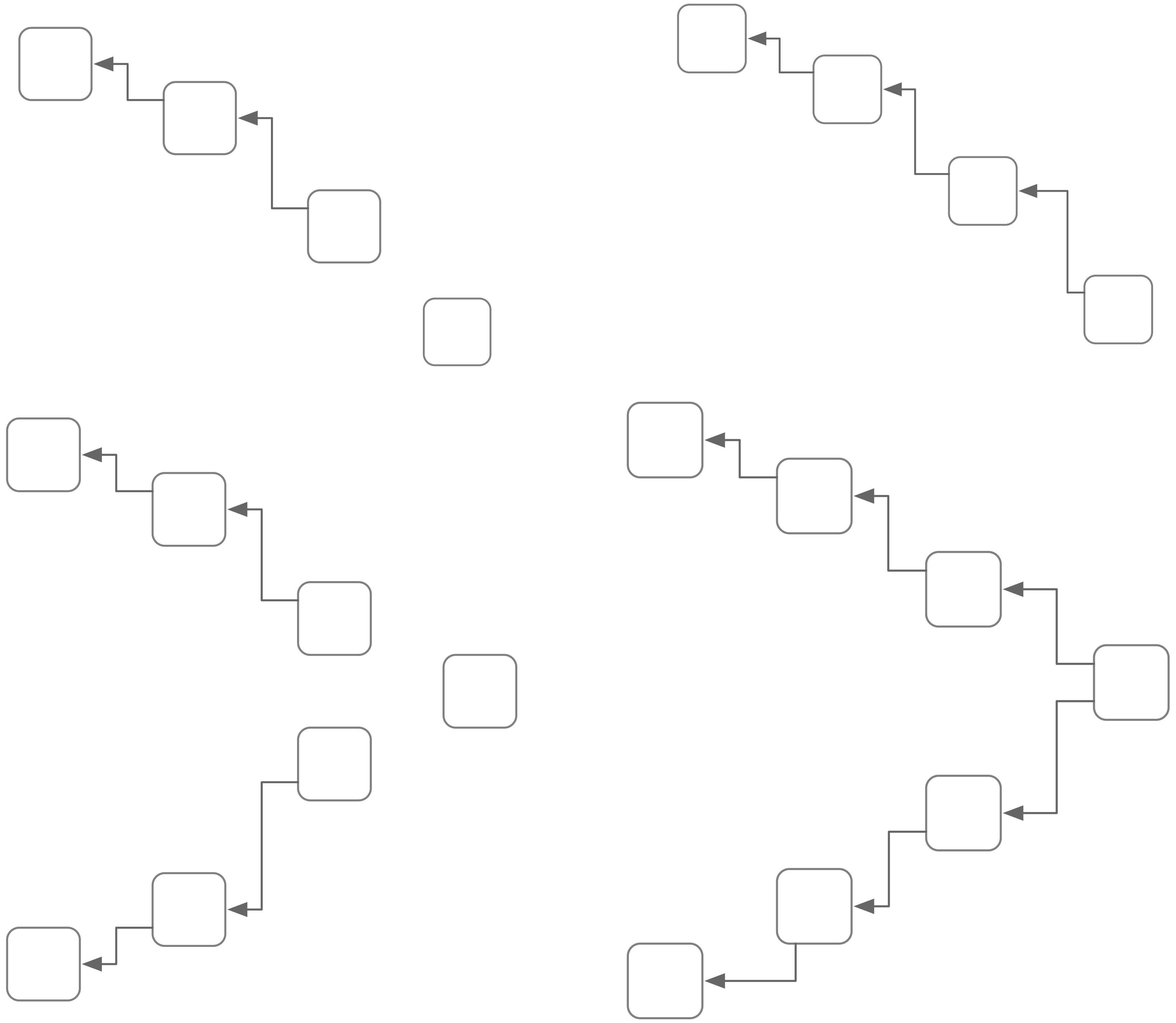
Chained ACDCs Enable

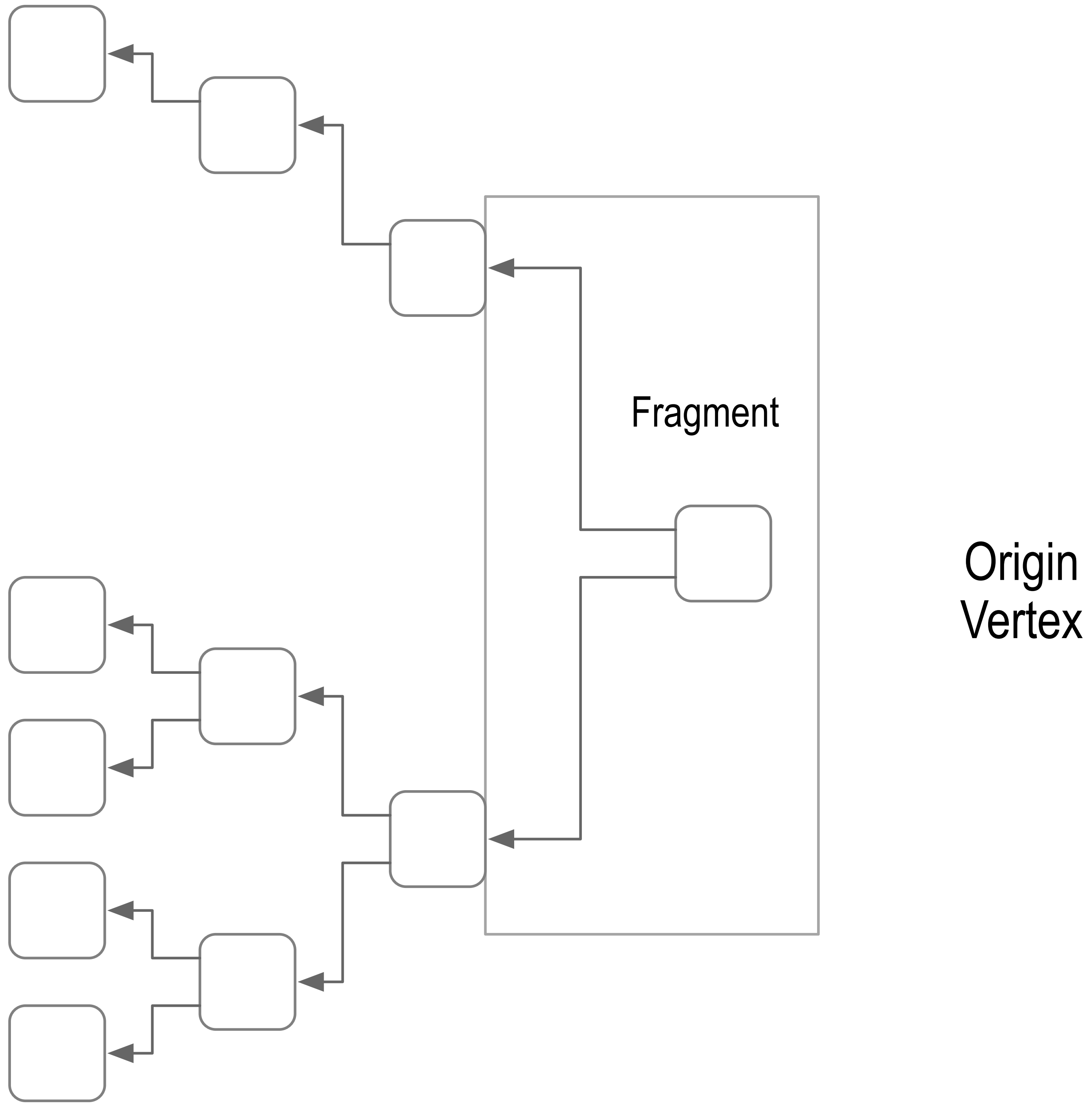
Provenanced chains-of-custody of decentralized authenticatable data attestations

Traceable data for data supply chains

Provenanced chains-of-authority for decentralized authenticatable credentials

Verifiable delegated entitlements or authorizations



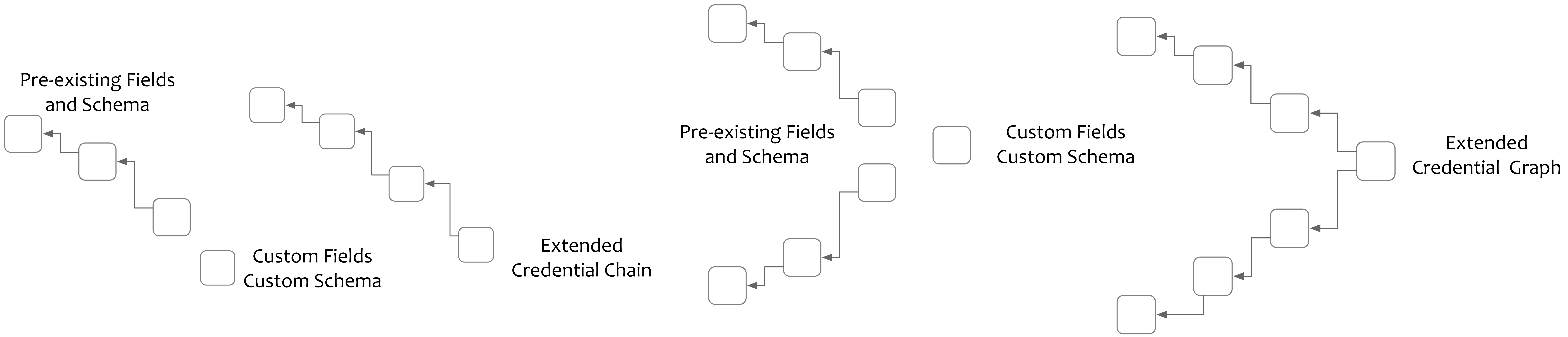


Append-to-Extend

Append-only verifiable data structures have strong security properties that simplify end-verifiability & foster decentralization.

Append-only provides permission-less extensibility by downstream issuers, presenters, and/or verifiers

- Each ACDC has a universally-unique content-based identifier with a universally-unique content-based schema identifier.
- Fully decentralized name-spacing.
- Custom fields are appended via chaining via one or more custom ACDCs defined by custom schema (type-is-schema).
- No need for centralized permissioned name-space registries to resolve name-space collisions.
- The purposes of a registry now become merely schema discovery or schema blessing for a given context or ecosystem.
- The reach of the registry is tuned to the reach of desired interoperability by the ecosystem participants.
- Human meaningful labels on SAIDs are local context only.
- Versioning is simplified because edges still verify if new schema are backwards compatible. (persistent data structure model)



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

GLEIF

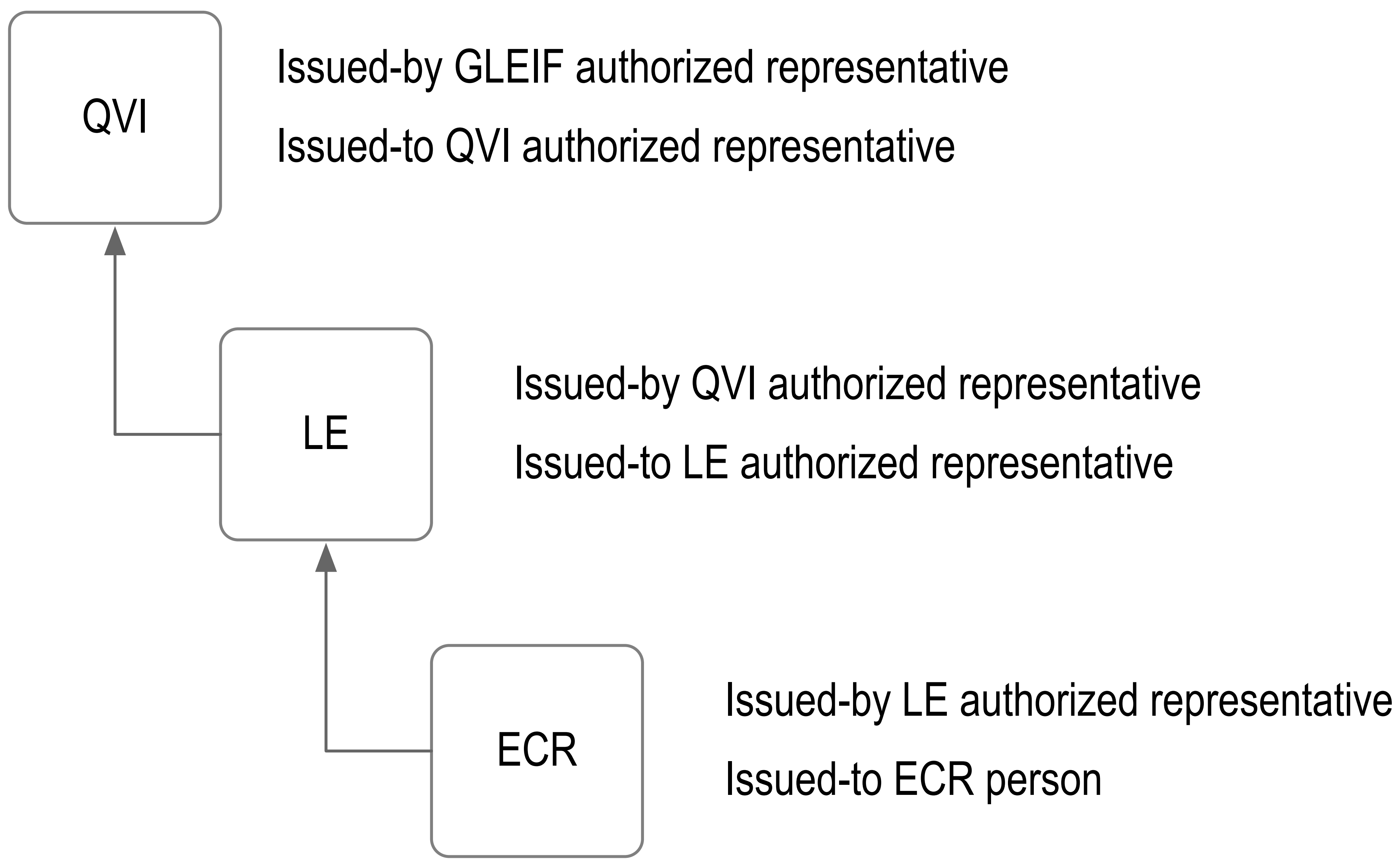
- **Qualified vLEI Issuers**
  - **Legal Entities**
    - **Persons Representing Legal Entities**

GLEIF vLEI Credential Example

Qualified vLEI Issuer (QVI) Credential

Legal Entity (LE) Credential

Engagement Context Role (ECR) Credential

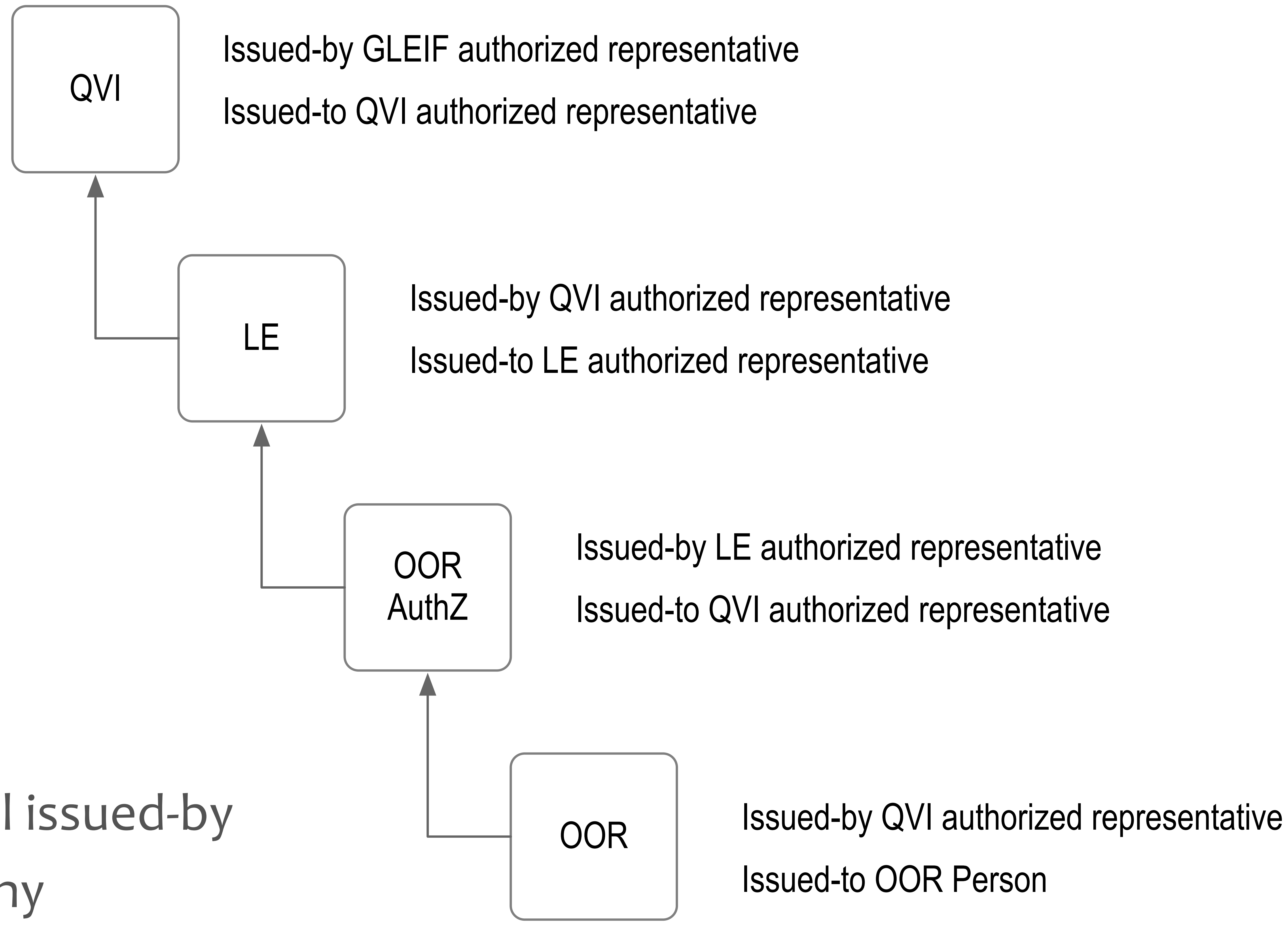


Qualified vLEI Issuer (QVI) Credential

Legal Entity (LE) Credential

Official Organizational Role Authorization (OOR-AuthZ) Credential

Official Organizational Role (OOR) Credential



Anyone in the chain-of-authority can revoke the credential issued-by them. This breaks the chain and thereby may invalidate any authorizations or attestations that are chained from their credential.

GLEIF vLEI Authorized Attestation Example

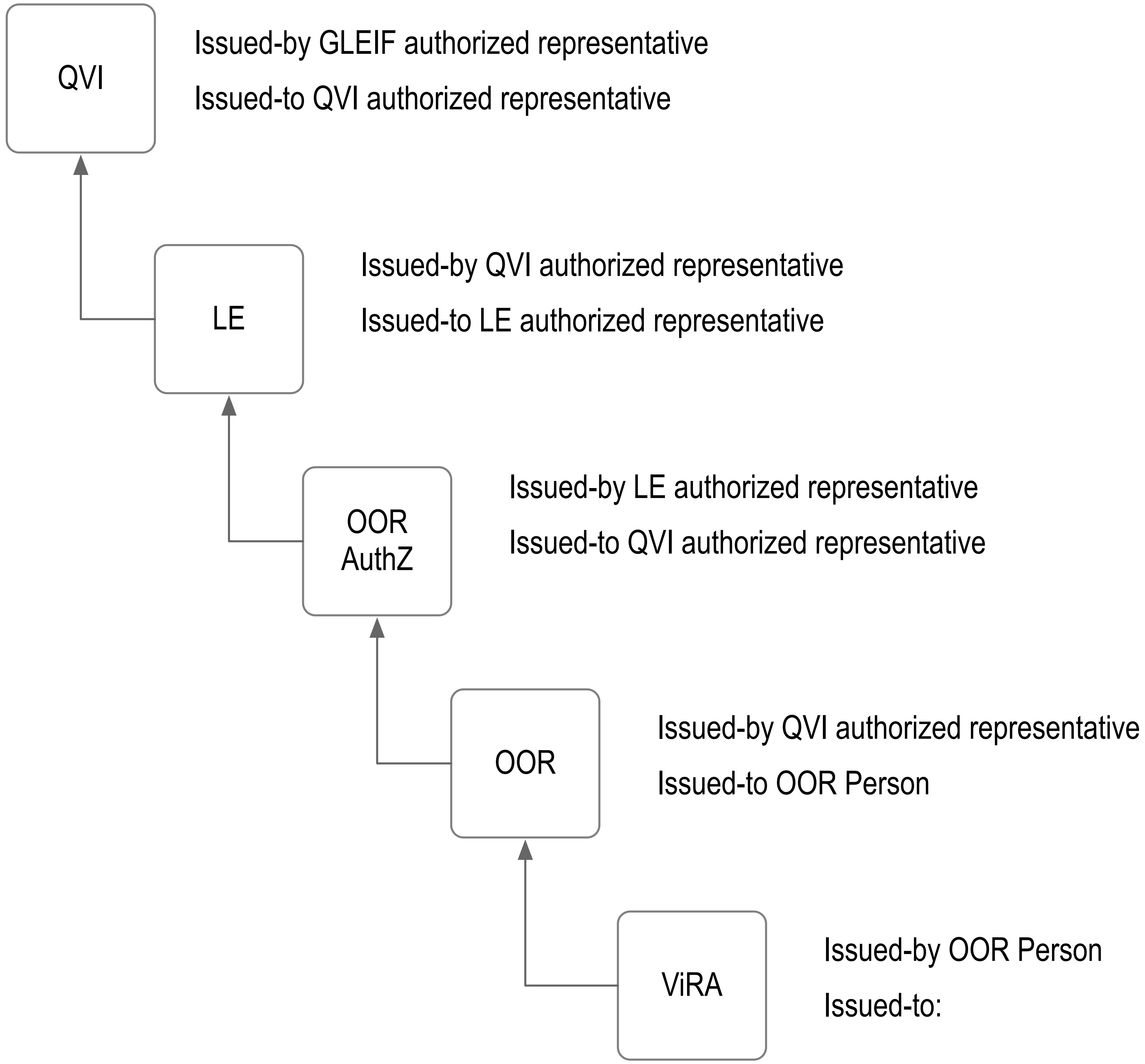
Qualified vLEI Issuer (QVI) Credential

Legal Entity (LE) Credential

Official Organizational Role Authorization (OOR-AuthZ) Credential

Official Organizational Role (OOR) Credential

Verifiable IXBRL Report Attestation (ViRA)



Anyone in the chain-of-authority can revoke the credential issued-by them. This breaks the chain and thereby may invalidate any authorizations or attestations that are chained from their credential.

IPEX Protocol

Enables graduated disclosure

IPEX Protocol

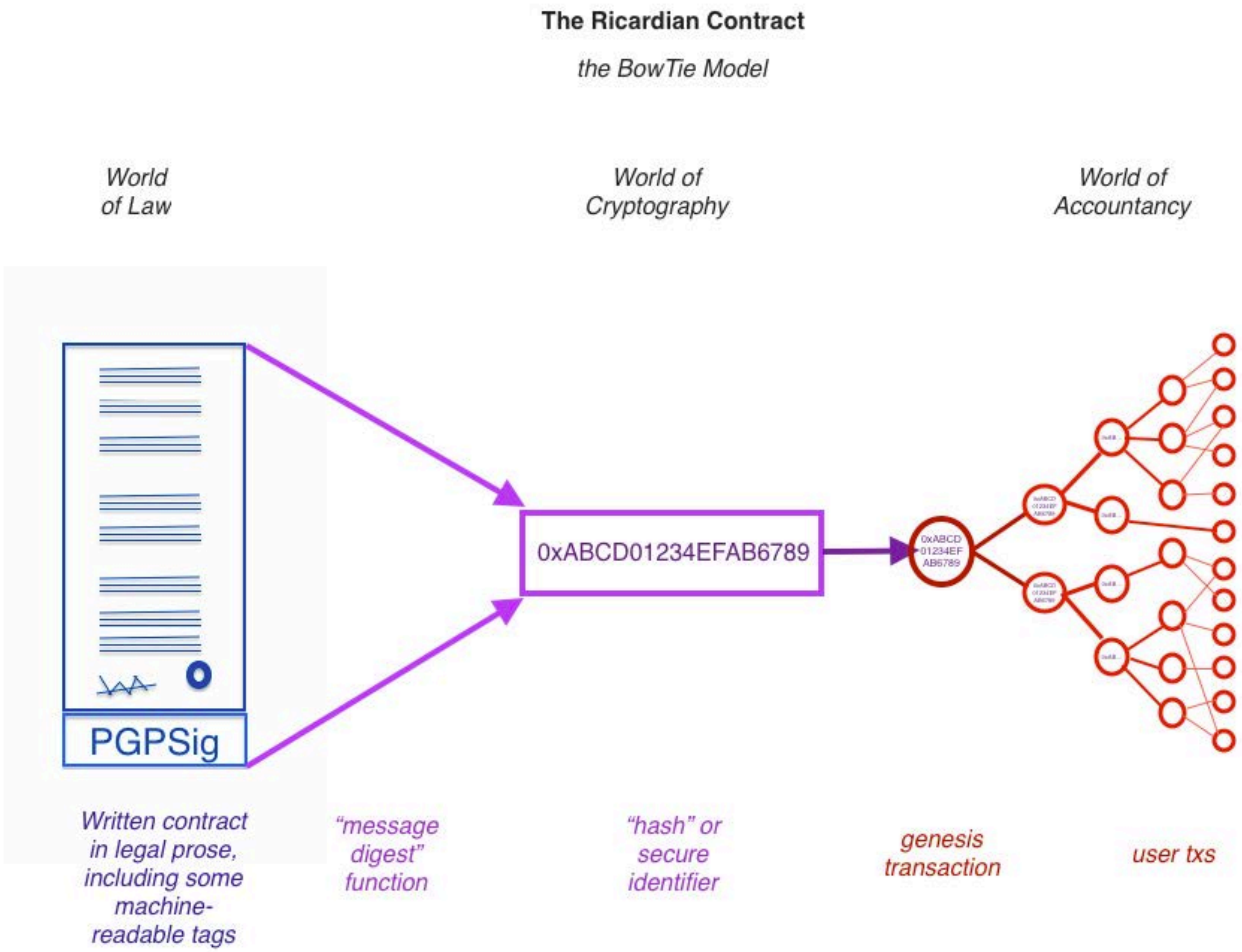
Discloser	Disclosee	Initiate	Contents	Description
	apply	Y	Schema or its SAID, Attribute field label list, Aggregate element label list, signature on *apply* or its SAID	proposes wanted disclosure
spurn		N		rejects *apply*
offer		Y	Metadata ACDC or its SAID, schema or its SAID, partial disclosure, Aggregate element label list, signature on offer or its SAID	proposes acceptable disclosure
	spurn	N		rejects *offer*
	agree	N	signature and/or anchored seal on offer or its SAID	accepts offer
spurn		N		rejects *agree*
grant		Y	Full or Selective Disclosure ACDC, signature on grant or its SAID	discloses agreed to offer
	admit	N	signature and/or anchored seal on grant or its SAID	confirms received grant disclosure

Contractually Protected Disclosure

Ricardian Contracts:
https://en.wikipedia.org/wiki/Ricardian_contract

Chain-link Confidentiality
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045818

Consent, Waiver, Terms-of-use, Remuneration, etc.



Chain-Link Confidentiality

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045818

A chain-link confidentiality regime contractually links the disclosure of information to obligations to protect that information as the information moves downstream.

The system focuses on the relationships not only between the discloser of information and the initial recipient but also between the initial recipient and subsequent recipients.

Through the use of contracts, this approach links recipients of information as in a chain, with each subsequent recipient bound by the same obligation to protect the information.

These chain contracts contain at least three kinds of terms:

1) obligations and restrictions on the use of the disclosed information;

2) requirements to bind future recipients to the same obligations and restrictions; and

3) requirements to perpetuate the contractual chain.

This approach creates a system for the permissible dissemination of information.

It protects Disclosers by ensuring that the recipient's obligation to safeguard information is extended to third parties.

Chain-Link Confidentiality

Disclosures via Presentations Exchanges may be contractually protected by Chain-Link Confidentiality (i.e a Chain-Link Confidential disclosure).

The chaining in this case is different from the chaining described above between Issuances in a DAG of chained Issuances. Chain-link confidentiality, in contrast, chains together a sequence of Disclosees.

Each Disclosee in the sequence in turn is the Discloser to the next Disclosee.

The terms-of-use of the original disclosure as applied to the original Disclosee MUST be applied by each subsequent Discloser to each subsequent Disclosee via each of the subsequent disclosures (presentation exchanges).

These terms-of-use typically constrain disclosure to only approved parties, i.e. imbue the chain of disclosures with some degree of confidentiality. These terms-of-use are meant to contractually protect the data rights of the original Issuer or Issuee of the data being disclosed.

Contractual Exchange

Discloser provides a non-repudiable ***Offer*** with verifiable metadata (sufficient partial disclosure), which includes any terms or restrictions on use.

Disclosee verifies ***Offer*** against composed schema and metadata adherence to desired data.

Disclosee provides non-repudiable ***Agree*** to terms that are contingent on compliant disclosure.

Discloser provides non-repudiable ***Grant*** disclosure with sufficient compliant detail.

Disclosee responds with ***Admit*** after verifying ***Grant*** using the decomposed schema and disclosed data.

Disclosee may now engage in permissioned use and carries liability as a deterrent against unpermissioned use.

ACDC Normative Field Labels

ACDC Field Labels

Label	Title	Description
		Top-level Fields
v	Version String	Regexable format: `ACDCMmmGggKKKKSSSS.` that provides protocol type, version, CESR genus version, serialization type, size, and terminator
t	Message Type	Three character message type when not default message type
d	Digest (SAID)	Self-referential fully qualified cryptographic digest of enclosing map.
u	UUID	Random Universally Unique IDentifier as fully qualified high entropy pseudo-random string, a salted nonce.
i	Identifier (AID)	Autonomic Identifier whose control authority is established via KERI verifiable Key State.
rd	Registry SAID	Registry for ACDC State.
s	Schema	Either the SAID of a JSON Schema block or the block itself.
a	Attribute	Either the SAID of a block of attributes or the block itself.
A	Aggregate	Either the Aggregate of a selectively disclosable block of attributes or the block itself.
e	Edge	Either the SAID of a block of edges or the block itself.
r	Rule	Either the SAID a block of rules or the block itself.
		Other Reserved Fields
d	Digest (SAID)	Self-referential fully qualified cryptographic digest of enclosing map.
u	UUID	Random Universally Unique IDentifier as fully qualified high entropy pseudo-random string, a salted nonce.
i	Identifier (AID)	Autonomic Identifier whose control authority is established via KERI verifiable Key State.
rd	Registry SAID	Registry for ACDC State.
dt	Datetime	Context dependent ISO datetime string
cargo	Cargo	Field value is embedded encapsulated data
n	Node	SAID of another ACDC as the terminating point of a directed edge that connects the encapsulating ACDC node to the specified ACDC node as a fragment of a distributed property graph (PG).
o	Operator	Either unary operator on edge or m-ary operator on edge-group in edge section. Enables expressing of edge logic on edge subgraph.
w	Weight	Edge weight property that enables default property for directed weighted edges and operators on directed weighted edges.
l	Legal Language	Text of Ricardian contract clause.

ACDC Example

Cal Registry Inception

```
{
  "v": “ACDCCAACAAJSONAADa.",
  "t": "rip",
  "d": "EPtolmh_NE2vC02oFc7FOiWkPcEiKUPWm5uu_Gv1JZDw",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXcy",
  "i": "ECsGDKWAYtHBCkiDrzajkxs3Iw2g-dls3bLUsRP4yVdT",
  "n": "0",
  "dt": "2025-07-04T17:52:00.000000+00:00"
}
```

Cal Issued Most Compact ACDC

```
{
  "v": "ACDCCAACAAJSONAAF3.",
  "t": "acm",
  "d": "EIF7egPvC8ITbGRdM9G0kd6aPELDg-azMkAqT-7cMuAi",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXdh",
  "i": "ECsGDKWAYtHBCkiDrzajkxs3Iw2g-dls3bLUsRP4yVdT",
  "rd": "EPtolmh_NE2vC02oFc7FOiWkPcEiKUPWm5uu_Gv1JZDw",
  "s": "EK_iGlfdc7Q-qIGL-kqbDSD2z4fesT4dAQLEHGgH4lLG",
  "a": "EK799owRYyk8UPFWUmfsm5AJfJmU7jZGtZXJFbg2I0KL",
  "r": "EMZf9m0XYwqo4L8tnIDMZuX7YCZnMswS7Ta9j0CuYfjU"
}
```

Cal Issued ACDC

```
{
  "v": "ACDCCAACAAJSONAAKX.",
  "t": "acm",
  "d": "EIF7egPvC8ITbGRdM9G0kd6aPELDg-azMkAqT-7cMuAi",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXdh",
  "i": "ECsGDKWAYtHBCkiDrzajkxs3Iw2g-dls3bLUsRP4yVdT",
  "rd": "EPtolmh_NE2vC02oFc7FOiWkPcEiKUPWm5uu_Gv1JZDw",
  "s": "EK_iGlfdc7Q-qIGL-kqbDSD2z4fesT4dAQLEHGgH4lLG",
  "a":
  {
    "d": "EK799owRYyk8UPFWUmfsm5AJfJmU7jZGtZXJFbg2I0KL",
    "u": "0ABhY2Rjc3BlY3dvcmtyYXc3",
    "i": "ECmiMVHTfZIjhA_rovnfx73T3G_FJzIQtzDn1meBVLAz",
    "name": "Sunspot College",
    "level": "gold"
  },
  "r":
  {
    "d": "EMZf9m0XYwqo4L8tnIDMZuX7YCZnMswS7Ta9j0CuYfjU",
    "l": "Issuer provides this ACDC on an AS IS basis. This ACDC in
whole or in part MUST NOT be shared with any other entity besides the
intended recipient."
  }
}
```

Cal ACDC Schema


```
{
  "$id": "EK_iGlfdc7Q-qIGL-
kqbDSD2z4fesT4dAQLEHGgH4lLG",
  "$schema": "https://json-schema.org/draft/2020-12/
schema",
  "title": "Accreditation Schema",
  "description": "Accreditation JSON Schema for acm
ACDC.",
  "credentialType": "Accreditation_ACDC_acm_message",
  "version": "2.0.0",
  "type": "object",
  "required": ["v", "d", "i", "s", "a", "r"],
  "properties":
  {
    "v": {"description": "ACDC version string", "type":
"string"},
    "t": {"description": "Message type", "type":
"string"},
    "d": {"description": "Message SAID", "type":
"string"},
    "u": {"description": "Message UUID", "type":
"string"},
    "i": {"description": "Issuer AID", "type":
"string"},
    "rd": {"description": "Registry SAID", "type":
"string"},
    "s":
    {
      "description": "Schema Section",
      "oneOf":
      [
          {"description": "Schema Section SAID",
"type": "string"},
          {"description": "Schema Section Detail",
"type": "object"}
      ]
    },
 …
```

```
   "a":
    {
      "description": "Attribute Section",
      "oneOf":
      [
        {"description": "Attribute Section SAID", "type":
"string"},
        {
          "description": "Attribute Section Detail",
          "type": "object",
          "required": ["d", "u", "i", "score", "name"],
          "properties":
          {
              "d": {"description": "Attribute Section SAID",
"type": "string"},
              "u": {"description": "Attribute Section UUID",
"type": "string"},
              "i": {"description": "Issuee AID", "type":
"string"},
              "name": {"description": "Institution Name",
"type": "string"},
              "level": {"description": "Accreditation Level",
"type": "string"}
          },
          "additionalProperties": false
        }
      ]
    },

        }
      ]
    }
  },
  "additionalProperties": false
…
```

```
    "e":
    {
      "description": "Edge Section",
      "oneOf":
      [
        {"description": "Edge Section SAID", "type": "string"},
        {"description": "Edge Section Detail", "type":
"object"}
      ]
    },
    "r":
    {
      "description": "Rule Section",
      "oneOf":
      [
        {"description": "Rule Section SAID", "type": "string"},
        {
          "description": "Rule Section Detail",
          "type": "object",
          "required": ["d", "l"],
          "properties":
          {
            "d": {"description": "Rule Section SAID", "type":
"string"},
            "l": {"description": "Legal Language", "type":
"string"}
          },
          "additionalProperties": false
        }
      ]
    }
  },
  "additionalProperties": false
}
```

ACDC Example …

Deb Registry Inception

```
{
  "v": "ACDCCAACAAJSONAADa.",
  "t": "rip",
  "d": "EJl5EUxL23p_pqgN3IyM-pzru89Nb7NzOM8ijH644xSU",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXcz",
  "i": "EEDGM_DvZ9qFEAPf_FX08J3HX49ycrVvYVXe9isaP5SW",
  "n": "0",
  "dt": "2025-07-04T17:53:00.000000+00:00"
}
```

Deb Issued Most Compact ACDC

```
{
  "v": "ACDCCAACAAJSONAAF3.",
  "t": "acm",
  "d": "EAU5dUws4ffM9jZjWs0QfXTnhJ1qk2u3IUhBwFVbFnt5",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXdi",
  "i": "EEDGM_DvZ9qFEAPf_FX08J3HX49ycrVvYVXe9isaP5SW",
  "rd": "EJl5EUxL23p_pqgN3IyM-pzru89Nb7NzOM8ijH644xSU",
  "s": "EKMXqyMQmOy0RuEj1VgOK9aD4GYR0D8Dcj0kssQtcY4-",
  "a": "EFTqnoiGSf-D76W3geNxEudBI_wz81FIkIXjzsjFztI-",
  "r": "EMZf9m0XYwqo4L8tnIDMZuX7YCZnMswS7Ta9j0CuYfjU"
}
```

Deb Issued ACDC

```
{
  "v": "ACDCCAACAAJSONAAK4.",
  "t": "acm",
  "d": "EAU5dUws4ffM9jZjWs0QfXTnhJ1qk2u3IUhBwFVbFnt5",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXdi",
  "i": "EEDGM_DvZ9qFEAPf_FX08J3HX49ycrVvYVXe9isaP5SW",
  "rd": "EJl5EUxL23p_pqgN3IyM-pzru89Nb7NzOM8ijH644xSU",
  "s": "EKMXqyMQmOy0RuEj1VgOK9aD4GYR0D8Dcj0kssQtcY4-",
  "a":
  {
    "d": "EFTqnoiGSf-D76W3geNxEudBI_wz81FIkIXjzsjFztI-",
    "u": "0ABhY2Rjc3BlY3dvcmtyYXc4",
    "title": "Post Quantum Security",
    "name": "Zoe Doe",
    "report": "Imprementation should prioritize cryptographic
agility over PQ."
  },
  "r":
  {
    "d": "EMZf9m0XYwqo4L8tnIDMZuX7YCZnMswS7Ta9j0CuYfjU",
    "l": "Issuer provides this ACDC on an AS IS basis. This ACDC
in whole or in part MUST NOT be shared with any other entity
besides the intended recipient."
  }
}
```

ACDC Example …

Bob Registry Inception

```
{
  "v": "ACDCCAACAAJSONAADa.",
  "t": "rip",
  "d": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXcx",
  "i": "ECWJZFBtllh99fESUOrBvT3EtBujWtDKCmyzDAXWhYmf",
  "n": "0",
  "dt": "2025-07-04T17:51:00.000000+00:00"
}
```

Bob Issued Most Compact ACDC

```
{
  "v": "ACDCCAACAAJSONAAF3.",
  "t": "acm",
  "d": "EMLjZLIMlfUOoKox_sDwQaJO-0wdoGW0uNbmI28Wwc4M",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXdj",
  "i": "ECWJZFBtllh99fESUOrBvT3EtBujWtDKCmyzDAXWhYmf",
  "rd": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
  "s": "EKMXqyMQmOy0RuEj1VgOK9aD4GYR0D8Dcj0kssQtcY4-",
  "a": "EIg1zAS3FfMMbQtLqARSwS3uGMttVbAPhKB71bjIPTs_",
  "r": "EMZf9m0XYwqo4L8tnIDMZuX7YCZnMswS7Ta9j0CuYfjU"
}
```

Bob Issued ACDC

```
{
  "v": "ACDCCAACAAJSONAAKt.",
  "t": "acm",
  "d": "EMLjZLIMlfUOoKox_sDwQaJO-0wdoGW0uNbmI28Wwc4M",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXdj",
  "i": "ECWJZFBtllh99fESUOrBvT3EtBujWtDKCmyzDAXWhYmf",
  "rd": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
  "s": "EKMXqyMQmOy0RuEj1VgOK9aD4GYR0D8Dcj0kssQtcY4-",
  "a":
  {
    "d": "EIg1zAS3FfMMbQtLqARSwS3uGMttVbAPhKB71bjIPTs_",
    "u": "0ABhY2Rjc3BlY3dvcmtyYXc5",
    "title": "PQ Proof of Concept",
    "name": "Zoe Doe",
    "report": "Demonstration of recovery from surprise quantum attack"
  },
  "r":
  {
    "d": "EMZf9m0XYwqo4L8tnIDMZuX7YCZnMswS7Ta9j0CuYfjU",
    "l": "Issuer provides this ACDC on an AS IS basis. This ACDC in whole or in part MUST NOT be shared with any other entity besides the intended recipient."
  }
}
```

ACDC Example …

Amy Registry Inception

```
{
  "v": "ACDCCAACAAJSONAADa.",
  "t": "rip",
  "d": "EOMMCyztOvg970W0dZVJT2JIwlQ22DSeY7wtxNBBtpmX",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXcw",
  "i": "ECmiMVHTfZIjhA_rovnfx73T3G_FJzIQtzDn1meBVLAz",
  "n": "0",
  "dt": "2025-07-04T17:50:00.000000+00:00"
}
```

Amy Issued Most Compact ACDC

```
{
  "v": "ACDCCAACAAJSONAAGg.",
  "d": "ENeNWgCCNcOf1JbgKxUzREKpyK5kABYFd2QYUzEfwz9H",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXdk",
  "i": "ECmiMVHTfZIjhA_rovnfx73T3G_FJzIQtzDn1meBVLAz",
  "rd": "EOMMCyztOvg970W0dZVJT2JIwlQ22DSeY7wtxNBBtpmX",
  "s": "EABGAia_vH_zHCRLOK3Bm2xxujV5A8sYIJbypfSM_2Fh",
  "a": "ELI2TuO6mLF0cR_0iU57EjYK4dExHIHdHxlRcAdO6x-U",
  "e": "ECpmTyIIc1duvCeIceK19Sbd0uymklmwNTtwtmfjQnX0",
  "r": "EMZf9m0XYwqo4L8tnIDMZuX7YCZnMswS7Ta9j0CuYfjU"
}
```

ACDC Example …

Amy Issued Registry


```
{
  "v": "ACDCCAACAAJSONAADa.",
  "t": "rip",
  "d": "EOMMCyztOvg970W0dZVJT2JIwlQ22DSeY7wtxNBBtpmX",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXcw",
  "i": "ECmiMVHTfZIjhA_rovnfx73T3G_FJzIQtzDn1meBVLAz",
  "n": "0",
  "dt": "2025-07-04T17:50:00.000000+00:00"
}
```


Amy Issued ACDC


```
{
  "v": "ACDCCAACAAJSONAAXG.",
  "d": "ENeNWgCCNcOf1JbgKxUzREKpyK5kABYFd2QYUzEfwz9H",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXdk",
  "i": "ECmiMVHTfZIjhA_rovnfx73T3G_FJzIQtzDn1meBVLAz",
  "rd": "EOMMCyztOvg970W0dZVJT2JIwlQ22DSeY7wtxNBBtpmX",
  "s": "EABGAia_vH_zHCRLOK3Bm2xxujV5A8sYIJbypfSM_2Fh",
  "a":
  {
    "d": "ELI2TuO6mLF0cR_0iU57EjYK4dExHIHdHxlRcAdO6x-U",
    "u": "0ABhY2Rjc3BlY3dvcmtyYXcw",
    "i": "ECWJZFBtllh99fESUOrBvT3EtBujWtDKCmyzDAXWhYmf",
    "name": "Zoe Doe",
    "gpa": 3.5,
    "grades":
    {
        "d": "EFQnBFeKAeS4DAWYoKDwWXOT4h2-XaGk7-w4-2N4ktXy",
        "u": "0ABhY2Rjc3BlY3dvcmtyYXcx",
        "history": 3.5,
        "english": 4.0,
        "math": 3.0
    }
  },
```


Amy Issued ACDC


```
 "e":
  {
    "d": "ECpmTyIIc1duvCeIceK19Sbd0uymklmwNTtwtmfjQnX0",
    "u": "0ABhY2Rjc3BlY3dvcmtyYXcy",
    "accreditation":
    {
        "d": "EAFj8JaNEC3mdFNJKrXW8E03_k9qqb_xM9NjAPVHw-xJ",
        "u": "0ABhY2Rjc3BlY3dvcmtyYXcz",
        "n": "EIF7egPvC8ITbGRdM9G0kd6aPELDg-azMkAqT-7cMuAi",
        "s": "EK_iGlfdc7Q-qIGL-kqbDSD2z4fesT4dAQLEHGgH4lLG"
    },
    "reports":
    {
        "d": "EOObmbCppe1S-7vtLuy766_4-RcfrC7p4ciFtBxdexuz",
        "u": "0ABhY2Rjc3BlY3dvcmtyYXc0",
        "o": "OR",
        "research":
        {
            "d": "EN9ngstOcFHqsjqf75JZFKtCRmW76NkeRrUSxTLoqqkI",
            "u": "0ABhY2Rjc3BlY3dvcmtyYXc2",
            "n": "EAU5dUws4ffM9jZjWs0QfXTnhJ1qk2u3IUhBwFVbFnt5",
            "o": "NI2I"
        },
        "project":
        {
            "d": "EFwHz5qJ4_8c7IefP7_zugX2eIgtoyY8Up_WZ3osXwkI",
            "u": "0ABhY2Rjc3BlY3dvcmtyYXc1",
            "n": "EMLjZLIMlfUOoKox_sDwQaJO-0wdoGW0uNbmI28Wwc4M",
            "o": "NI2I"
        }
    }
  },
  "r":
  {
    "d": "EMZf9m0XYwqo4L8tnIDMZuX7YCZnMswS7Ta9j0CuYfjU",
    "l": "Issuer provides this ACDC on an AS IS basis. This ACDC in whole or in part MUST NOT be shared with any other entity besides the intended recipient."
  }
}
```

ACDC Selective Disclosure Example

Aggregate Section

```
"A":
[
  "EN5d44fTNM0M4kmMMVrsH0HwMLRLyb6SoJEV0ogkLdXx",
  {
      "d": "EI2lwi1ZKrs-bDwgEreOhEh-W2O5xrOm5T-QCyMuX5V4",
      "u": "0ABhY2Rjc3BlY3dvcmtyYXcw",
      "i": "ECWJZFBtllh99fESUOrBvT3EtBujWtDKCmyzDAXWhYmf"
  },
  {
      "d": "EC-vU19URXX8ztfWdp_j2HHr1lJsqtGa1YHtZrg6-GMR",
      "u": "0ABhY2Rjc3BlY3dvcmtyYXcx",
      "score": 96
  },
  {
      "d": "EKYLUIpDXNT0ujSdoNOT5pLp0okOKW3mAbg-M7K5OO_C",
      "u": "0ABhY2Rjc3BlY3dvcmtyYXcy",
      "name": "Zoe Doe"
  }
]
```

Blinded Aggregate Element List

```
"A":
[
  "EN5d44fTNM0M4kmMMVrsH0HwMLRLyb6SoJEV0ogkLdXx",
  "EI2lwi1ZKrs-bDwgEreOhEh-W2O5xrOm5T-QCyMuX5V4",
  "EC-vU19URXX8ztfWdp_j2HHr1lJsqtGa1YHtZrg6-GMR",
  "EKYLUIpDXNT0ujSdoNOT5pLp0okOKW3mAbg-M7K5OO_C"
]
```

AGID = H(C(a_i for all i in \{0, ..., N\})), where

H is the digest (hash) Operator and

C is the ordered serialization operator.

This aggregate AGID makes a blinded cryptographic commitment to all SAIDS in the list [a_1, …, a_N].

"A": “EN5d44fTNM0M4kmMMVrsH0HwMLRLyb6SoJEV0ogkLdXx"

ACDC Selective Disclosure Example …

Selectively Disclosed Aggregate Section


```
"A":
[
  "EN5d44fTNM0M4kmMMVrsH0HwMLRLyb6SoJEV0ogkLdXx",
  {
    "d": "EI2lwi1ZKrs-bDwgEreOhEh-W2O5xrOm5T-QCyMuX5V4",
    "u": "0ABhY2Rjc3BlY3dvcmtyYXcw",
    "i": "ECWJZFBtllh99fESUOrBvT3EtBujWtDKCmyzDAXWhYmf"
  },
  {
    "d": "EC-vU19URXX8ztfWdp_j2HHr1lJsqtGa1YHtZrg6-GMR",
    "u": "0ABhY2Rjc3BlY3dvcmtyYXcx",
    "score": 96
  },
  "EKYLUIpDXNT0ujSdoNOT5pLp0okOKW3mAbg-M7K5OO_C"
]
```

ACDC Blinded Registry Example

Registry Inception


```
{
 "v": "ACDCCAACAAJSONAADa.",
  "t": "rip",
  "d": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXcx",
  "i": "ECWJZFBtllh99fESUOrBvT3EtBujWtDKCmyzDAXWhYmf",
  "n": "0",
  "dt": "2025-07-04T17:51:00.000000+00:00"
}
```


Registry Placeholder Update


```
{
  "v": "ACDCCAACAAJSONAAEi.",
  "t": "bup",
  "d": "EPNwyvHp2XJsz9pSpXtHtcCmzw6bKSFc-nhGKTbso0Yg",
  "rd": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
  "n": "1",
  "p": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
  "dt": "2025-08-01T18:06:10.988921+00:00",
  "b": "ECVr7QWEp_aqVQuz4yprRFXVxJ-9uWLx_d6oDinlHU6J"
}
```


Virtual Label	Value	Description
`d`	`ECVr7QWEp_aqVQuz4yprRFXVxJ-9uWLx_d6oDinlHU6J`	BLID (Blinding SAID)
`u`	`aG1lSjdJSNl7TiroPl67Uqzd5eFvzmr6bPlL7Lh4ukv8`	UUID salty nonce blinding factor, random or HD generated
`td`	`1AAP`	Transaction ACDC SAID field value, top-level `d`
`ts`	`1AAP`	Transaction state value string

Unblinded attribute block as attachment to disclosure of TEL Event

`-aAYECVr7QWEp_aqVQuz4yprRFXVxJ-9uWLx_d6oDinlHU6JaG1lSjdJSNl7TiroPl67Uqzd5eFvzmr6bPlL7Lh4ukv81AAP1AAP`

Placeholder updates provide herd privacy wrt correlation to date time of actual state changes

ACDC Blinded Registry Example ...

Registry Issued Update


```
{
  "v": "ACDCCAACAAJSONAAEi.",
  "t": "bup",
  "d": "EBdytzDC4dnatn-6mrCWLSGuM62LM0BgS31YnAg5NTeW",
  "rd": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
  "n": "2",
  "p": "EPNwyvHp2XJsz9pSpXtHtcCmzw6bKSFc-nhGKTbso0Yg",
  "dt": "2020-08-02T12:00:20.000000+00:00",
  "b": "EOtWw6X_aoOJlkzNaLj23IC6MXHl7ZSYSWVulFW_Hr_t"
}
```


Virtual Label	Value	Description
`d`	`EOtWw6X_aoOJlkzNaLj23IC6MXHl7ZSYSWVulFW_Hr_t`	Dummied BLID (Blinding SAID)
`u`	`aLfCdNAnc-0P2SiruarZSajXiUWu5iU2VfQahvpNCyzB`	UUID salty nonce blinding factor, random or HD generated
`td`	`EMLjZLIMlfUOoKox_sDwQaJO-0wdoGW0uNbmI28Wwc4M`	Transaction ACDC SAID field value, top-level `d`
`ts`	`0Missued`	Transaction state value string

ACDC Blinded Registry Example …

Registry Issued Update


```json
{
    "v": "ACDCCAACAAJSONAAEi.",
    "t": "bup",
    "d": "EM8B1uDhWaJLfpIiEqgp-3EurGUcbfe7u2k5AarDl2XD",
    "rd": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
    "n": "3",
    "p": "EBdytzDC4dnatn-6mrCWLSGuM62LM0BgS31YnAg5NTeW",
    "dt": "2020-08-03T12:00:20.000000+00:00",
    "b": "EPj3sZj8OOWTkTgAN5vzVYdANeoj3zxgEn5APb8fCRRN"
}
```


Virtual Label	Value	Description
d	EPj3sZj8OOWTkTgAN5vzVYdANeoj3zxgEn5APb8fCRRN	Dummied BLID (Blinding SAID)
u	aGx7b16vGHVPT56tX30kYOEzTwiVY4aabc4k9AawYyZG	UUID salty nonce blinding factor HD generated
td	EMLjZLIMlfUOoKox_sDwQaJO-0wdoGW0uNbmI28Wwc4M	Transaction ACDC SAID field value, top-level d
ts	Yrevoked	Transaction state value string

ACDC Bound Blinded Registry Example

Registry Inception

```
{
 "v": "ACDCCAACAAJSONAADa.",
  "t": "rip",
  "d": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
  "u": "0ABhY2Rjc3BlY3dvcmtyYXcx",
  "i": "ECWJZFBtllh99fESUOrBvT3EtBujWtDKCmyzDAXWhYmf",
  "n": "0",
  "dt": "2025-07-04T17:51:00.000000+00:00"
}
```

Registry Placeholder Update

```
{
    "v": "ACDCCAACAAJSONAAEi.",
    "t": "bup",
    "d": "EOBVdcIL2rVEzBDpQvmBpsp3R52DsoKhTAAdvHqAz9yc",
    "rd": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
    "n": "1",
    "p": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
    "dt": "2025-08-01T18:06:10.988921+00:00",
    "b": "EFaQ00QW-ZeoMxE9baWcpJbAFXrs5h0ya-wpKnHvMQ0c"
}
```

Virtual Label	Value	Description
d	EFaQ00QW-ZeoMxE9baWcpJbAFXrs5h0ya-wpKnHvMQ0c	BLID (Blinding SAID)
u	aJxtoz6qVeJxPCZvP-qBJifRfIxP3itQBVAAu7JJHxMa	UUID salty nonce blinding factor, HD generated
td	1AAP	Transaction ACDC SAID field value, top-level d
ts	1AAP	Transaction state value string
bn	MAAA	Bound Issuee key event sequence number field
bd	1AAP	Bound Issuee key event SAID field

Unblinded attribute block as attachment to disclosure of TEL Event

`-bAaEFaQ00QW-ZeoMxE9baWcpJbAFXrs5h0ya-wpKnHvMQ0caJxtoz6qVeJxPCZvP-qBJifRfIxP3itQBVAAu7JJHxMa1AAP1AAPMAAA1AAP`

Placeholder updates provide herd privacy wrt correlation to date time of actual state changes

ACDC Bound Blinded Registry Example ...

Registry Issued Update


```
{
    "v": "ACDCCAACAAJSONAAEi.",
    "t": "bup",
    "d": "EGu4B78s6G_GVrzaoBw2a1vkFpB5tVo-wZ1OGsC9D_pK",
    "rd": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
    "n": "2",
    "p": "EOBVdcIL2rVEzBDpQvmBpsp3R52DsoKhTAAdvHqAz9yc",
    "dt": "2020-08-02T12:00:20.000000+00:00",
    "b": "EJAeKLEtVtMtt28IdAKJShyZHodEIZTHJHzaP21A_ZU4"
}
```


Virtual Label	Value	Description
d	EJAeKLEtVtMtt28IdAKJShyZHodEIZTHJHzaP21A_ZU4	BLID (Blinding SAID)
u	aKNPEY4_60x6vUx2g5_5kAoJTn0RDspR04Ql8ecNyTkO	UUID salty nonce blinding factor, HD generated
td	EMLjZLIMlfUOoKox_sDwQaJO-0wdoGW0uNbmI28Wwc4M	Transaction ACDC SAID field value, top-level d
ts	0Missued	Transaction state value string
bn	MAAB	Bound Issuee key event sequence number field
bd	EJOnAKXGaSyJ_43kit0V806NNeGWS07lfjybB1UcfWsv	Bound Issuee key event SAID field

Unblinded attribute block as attachment to disclosure of TEL Event

-bAvEJAeKLEtVtMtt28IdAKJShyZHodEIZTHJHzaP21A_ZU4aKNPEY4_60x6vUx2g5_5kAoJTn0RDspR04Ql8ecNyTkOEMLjZLIMlfUOoKox_sDwQaJO-0wdoGW0uNbmI28Wwc4M0MissuedMAABEJOnAKXGaSyJ_43kit0V806NNeGWS07lfjybB1UcfWsv

ACDC Bound Blinded Registry Example ...

Registry Issued Update

```
{
    "v": "ACDCCAACAAJSONAAEi.",
    "t": "bup",
    "d": "EDXGqM-V_sfj65Dk-lgMnpOZ9DYziqMaYkrju7NRKpFn",
    "rd": "ECOWJI9kAjpCFYJ7RenpJx2w66-GsGlhyKLO-Or3qOIQ",
    "n": "3",
    "p": "EGu4B78s6G_GVrzaoBw2a1vkFpB5tVo-wZ1OGsC9D_pK",
    "dt": "2020-08-03T12:00:20.000000+00:00",
    "b": "EIBNZ3t5rA_-PbBNmhtvtf0VgHBjVrE0fc-DO67f-wGv"
}
```

Virtual Label	Value	Description
d	EIBNZ3t5rA_-PbBNmhtvtf0VgHBjVrE0fc-DO67f-wGv	BLID (Blinding SAID)
u	aFudXE-d0b2owzZNBjd78sx4kCTJx-RTP_Zd19HRUcVD	UUID salty nonce blinding factor, HD generated
td	EMLjZLIMlfUOoKox_sDwQaJO-0wdoGW0uNbmI28Wwc4M	Transaction ACDC SAID field value, top-level d
ts	Yrevoked	Transaction state value string
bn	MAAI	Bound Issuee key event sequence number field
bd	EDeCPBTHAt75Acgi9PfEciHFnc1r2DKAno3s9_QIYrXk	Bound Issuee key event SAID field

Unblinded attribute block as attachment to disclosure of TEL Event

-bAvEIBNZ3t5rA_-PbBNmhtvtf0VgHBjVrE0fc-DO67f-wGvaFudXE-d0b2owzZNBjd78sx4kCTJx-
RTP_Zd19HRUcVDEMLjZLIMlfUOoKox_sDwQaJO-0wdoGW0uNbmI28Wwc4MYrevokedMAAIEDeCPBTHAt75Acgi9PfEciHFnc1r2DKAno3s9_QIYrXk

ACDC Bulk Issuance with full cryptographic unlinkability validator to validator

The UUIDs in each member of a bulk-issued set are derived using an HDKey algorithm whose path contains a shared secret salt, the member index, and the UUID index.

Each member of a bulk-issued set has a unique AID with unique keys derived using an HDKey algorithm whose path contains a shared secret salt, the member index, and a non-shared private salt.

When using *independent registry bulk-issued ACDCs*, the total number of registries for a given set of bulk-issued ACDCs is equal to the number of members of the set.

All the seals are anchored using a single seal, which is the Merkle root of a Sparse Merkle tree that references the transaction events for all the independent Registry TELs.

In a Sparse Merkle tree, the seals are only stored in leaf nodes of the tree, not in intermediate nodes [61].

Sparse Merkle trees (SMTs) were originally developed for the Certificate Transparency (CT) network.

Since then, various optimized versions of SMT have been developed, including the CT Trillian Tessera (tile-based SMT) [62][63][64][65] [66][67][68].

The efficient inclusion proofs of an SMT enable a given Issuer to amalgamate all Registry transaction event seals for all its bulk-issued ACDCs into a single SMT.

This provides so-called herd privacy to the updates.

To further strengthen herd privacy, when using blindable state Registries, the Issuer could randomly issue update events that do not change state, across all its registries, mixing updates over time and across each registry.

This would ensure that enough updates are captured by each batch anchoring seal to guarantee a pre-specified level of herd privacy.

A given seal in the KEL of the Issuer no longer provides a point of correlation to any other transaction event to any given registry.

A given inclusion proof for one event from one Registry does not reveal inclusion for events in other Registries or correlate a given bulk-issued ACDC to any other bulk-issued ACDC using a different Registry.

This amalgamation requires only one seal in the Issuer's KEL.

Using an optimized SMT algorithm enables an Issuer to provide efficient inclusion proofs for an amalgamated SMT of all transaction update events across all Registries for all bulk-issued ACDCs to all Issuees.

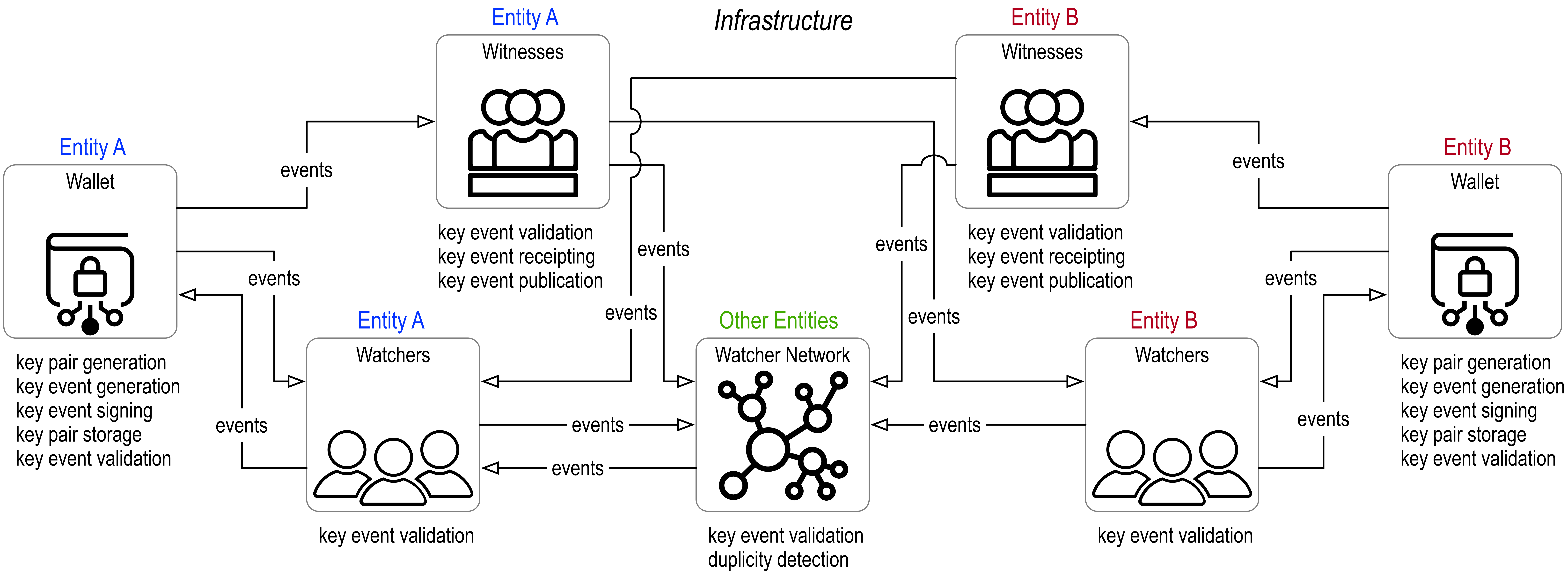
When using blindable state update events in these Registries, then the ACDC is not viewable by a 3rd party.

Because the SMT provides herd privacy with respect to which Registries with their transaction event updates belong to which bulk-issued sets of ACDCS, a pair of malicious 2nd parties cannot compare inclusion proofs to determine if two ACDCs belong to the same bulk-issued set.

Moreover, because each ACDC in a bulk-issued set gets its own Registry, the registry database does not provide a point of correlation between two different Registries that belong to the same bulk-issued set of ACDCs.

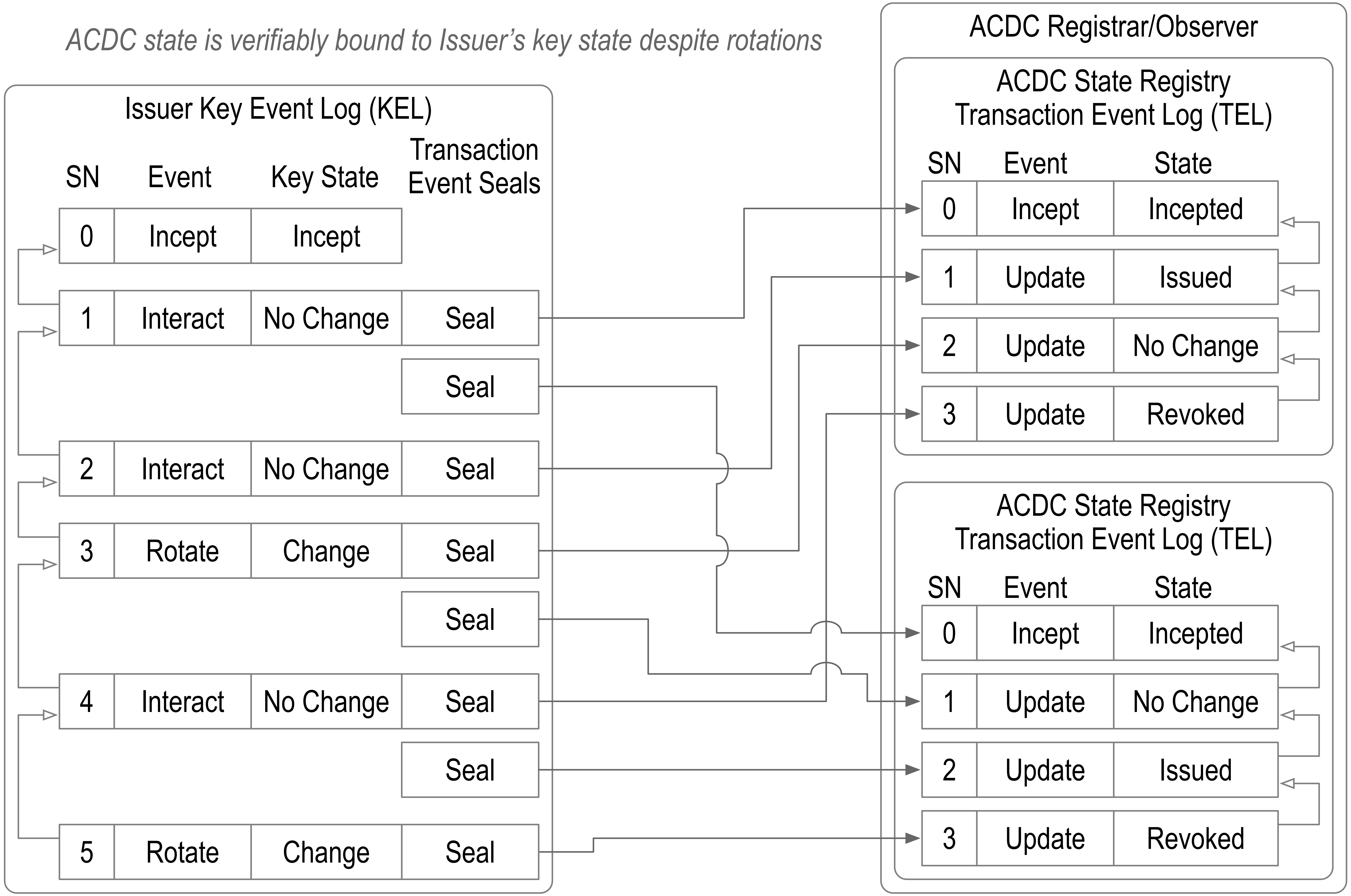
Therefore, a given disclosure of a bulk-issued ACDC does not directly disclose any points of correlation between malicious 2nd parties.

KERI Ecosystem



ACDC State Registry using Transaction Event Log (TEL)

Each Transaction Event is bound to Issuer key stated via anchoring seal in Issuers KEL



Registars and Observers

A TEL Registrar operates under the auspices of the ACDC Issuer to maintain and publish a Registry of the ACDC state via a TEL.

A point of validation (PoV) occurs when an ACDC is presented to a Validator for validation.

A TEL Observer operates under the auspices of one or more Validators to cache the Registry, allowing Validators to validate the state of a given ACDC without exposing a point of validation (PoV).

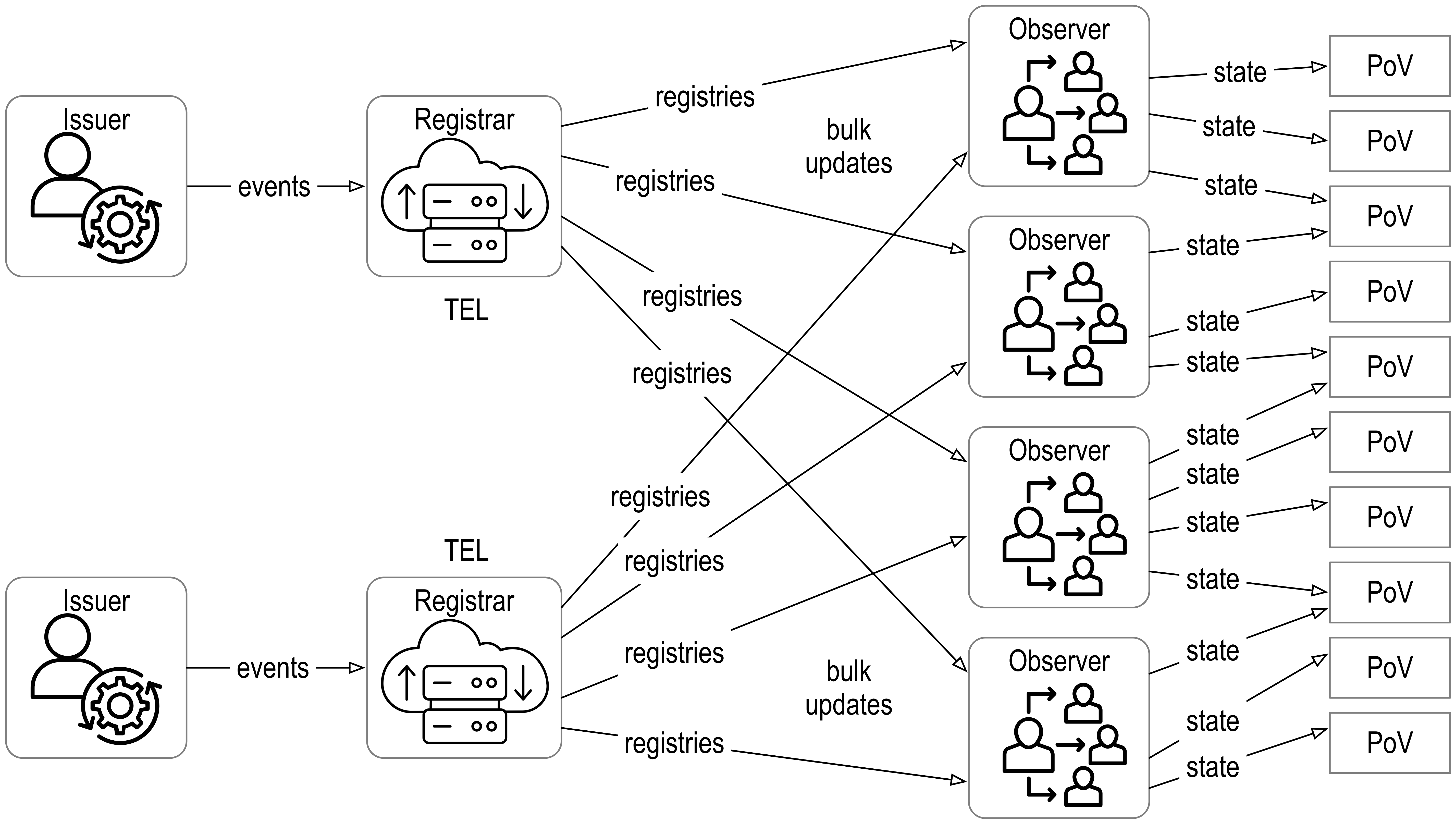
Observers maintain an updated cache of the Registry, reflecting bulk ACDC Registry state updates provided by the Registrar.

Observers mask the usage of a given ACDC from the Issuer.

A Validator queries its Observer, not the Registrar, at a point of validation (PoV) for an ACDC.

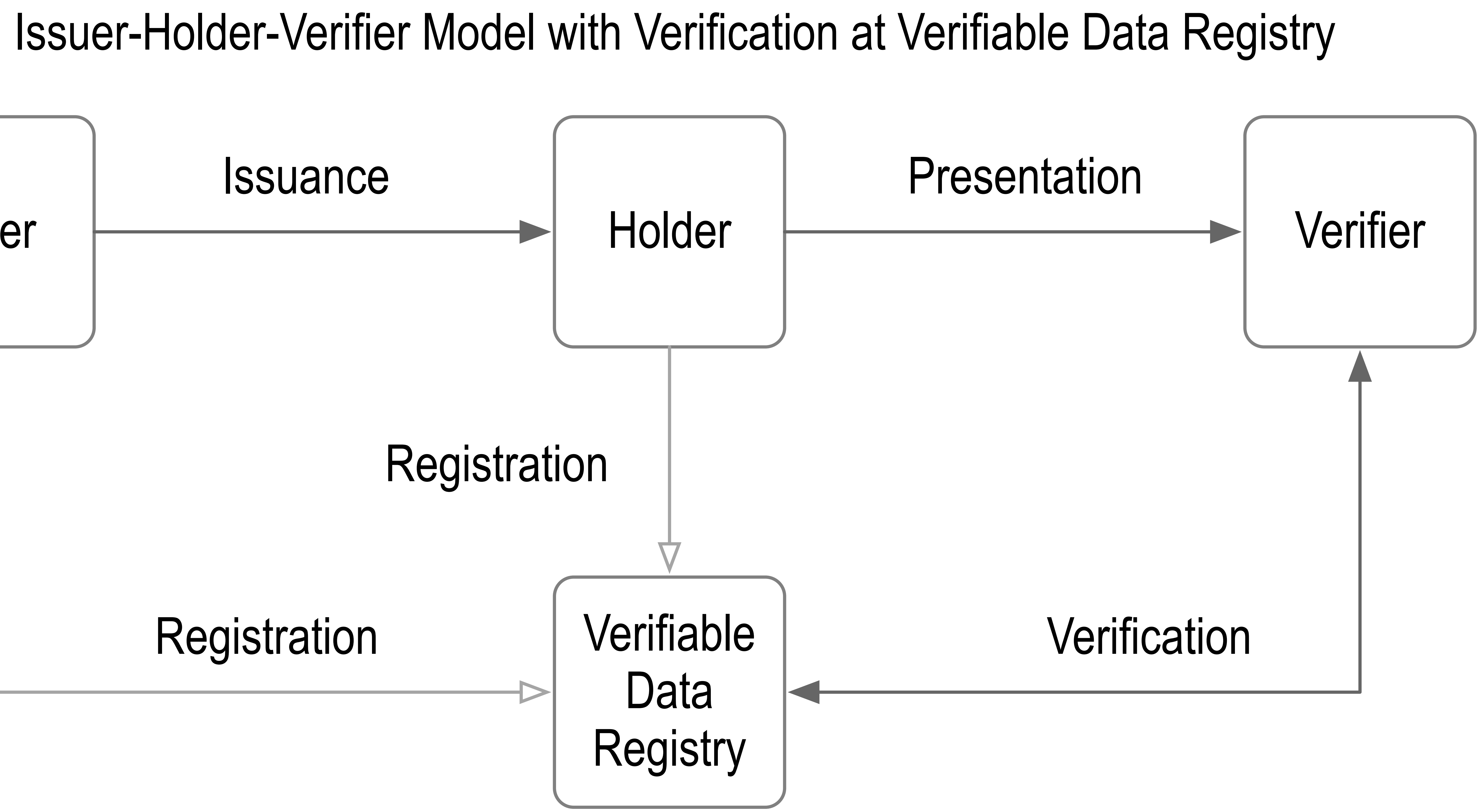
Interactions between the Observer and Registrar occur at bulk ACDC Registry state changes, not at the PoV of a given ACDC state.

This protects against forced validator-to-issuer correlation of ACDC usage, i.e., no forced phone home validation.

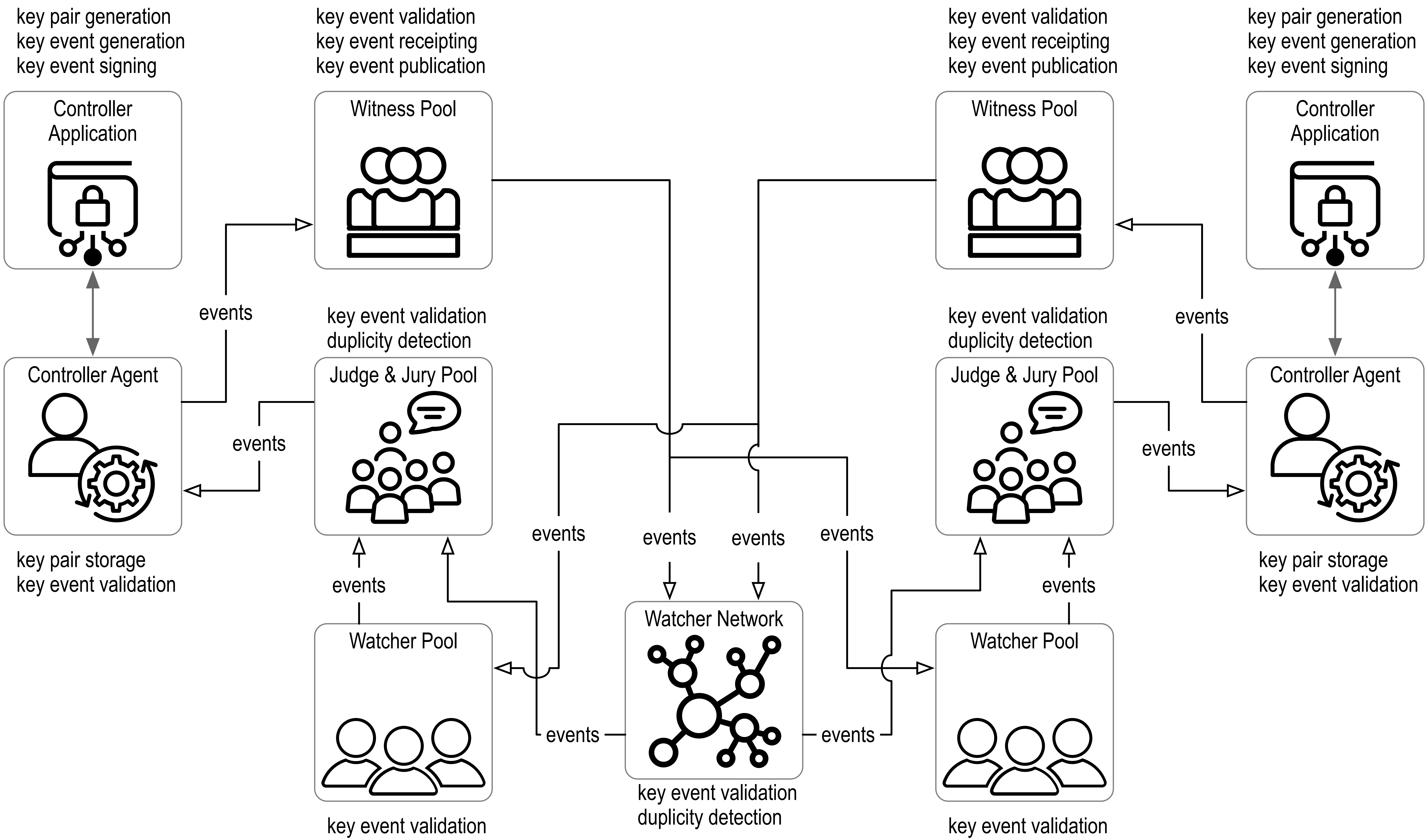


Open-Loop Tripartite Model

Verifiable Data Registry (VDR) enables decentralized but interoperable discovery and verification of Issuance state.

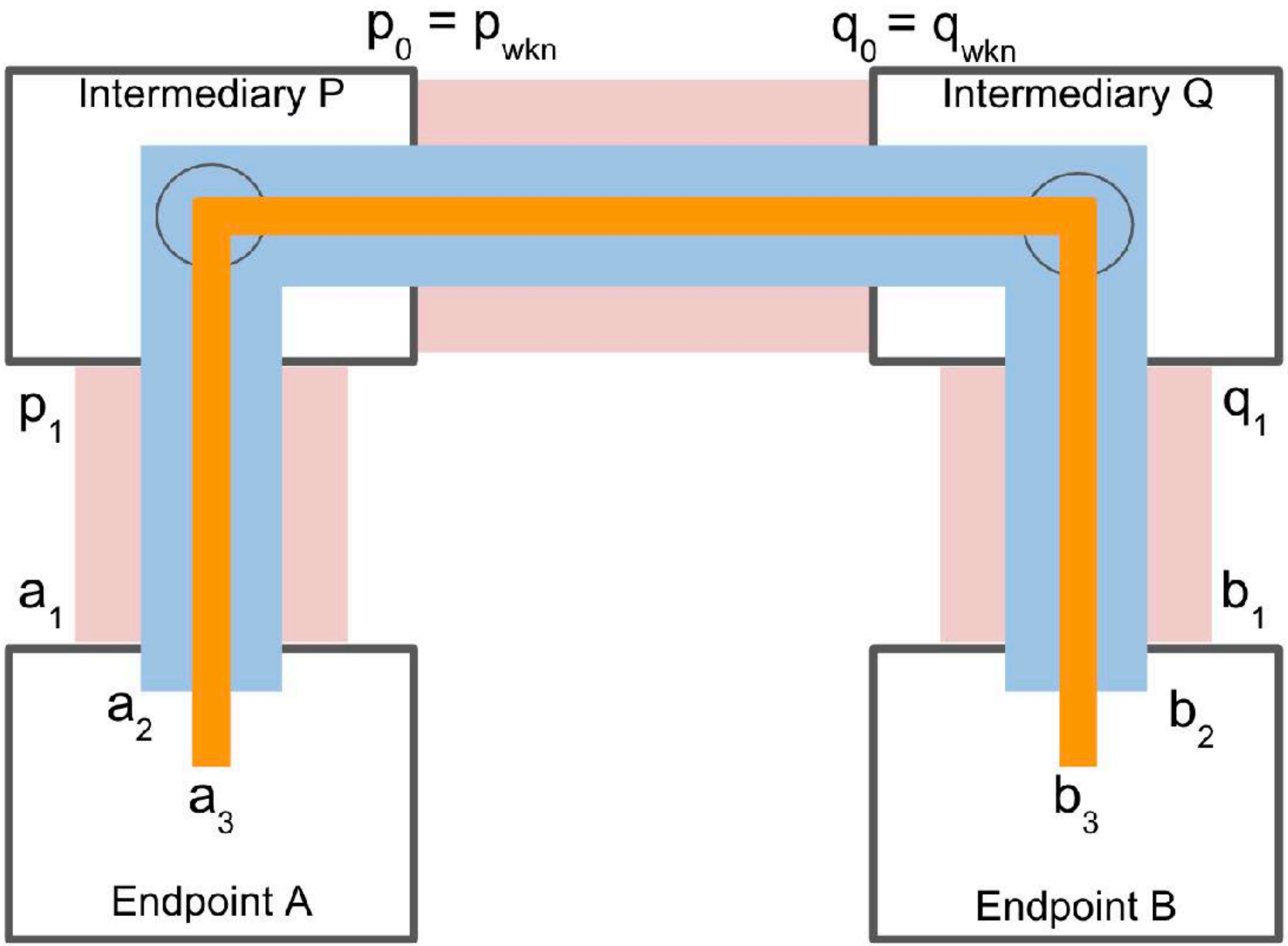


KERI Ecosystem



TSP (SPAC) Protocol

Triple-nested tunneling protocol that minimizes surveillable metadata



covert vs. clandestine surveillability

Reputable Authenticatable Pseudonymity (RAP)

Reputation is a behavior-based contextual predictor that enables an interaction.

RAP = Trust based on contextual behavior that is securely cryptonymously attributable but without linkage to an actual person or legal entity.

The corpus of breaches, combined with tooling that enables ambient correlatability of everyone in the current ecosystem to that corpus, means that there is no practical pseudonymity without strong counterincentives for 2nd parties to share contextual behavior data.

TSP/SPAC protects against direct third-party surveillance/correlation of metadata.

Granular Partitioning of Data-Sharing Contexts

The Trust over IP (ToIP) is developing a protocol called the Trust Spanning Protocol (TSP) that granularly partitions data-sharing contexts so that correlatability is also granularly partitioned.

The TSP protocol enables one to control the exploitable time value of the correlatable information that can be leaked from a given context.

Once a context has become leaky, a new isolated context can be created that restarts the clock on time-value correlatability.

This provides a trade-space between:

- the friction and cost of forming and maintaining contexts
- the length of time before a given context becomes leaky
- the time constant of the exploitable value of leaked information.

If the leakiness of a given context is cost-effectively protectable beyond the time constant on the time value of exploitation, then new information is sustainably protectable indefinitely.

Contexts and Sustainable Privacy

Sustainable Management of Contexts

A party wishing to protect against exploitation via correlatable metadata (identifiers) sustainably has a similar problem to that of the operatives in covert and/or clandestine operations.

Covert: A covert operation is an operation that is planned and executed in secrecy so that the identity of the agency or organization remains unknown or is plausibly deniable.

Clandestine: A clandestine operation is an operation that is carried out in such a manner that the operation remains in secrecy or is concealed.

From the standpoint of a covert operative, the fact that the organization conducting the operation remains unknown puts the operative at great risk. The organization can burn or disavow the operative without incurring liability to the organization itself. This means the operative must have a legitimate public cover identity.

Whereas a clandestine operative has no such public cover, should the operative be discovered then that discovery would incur liability to the orgainzation itself. This means clandestine operations have more limited use cases that are constrained by the technical and operative challenges of maintaining the privacy of the whole operation, including all operatives.

Consequently, covert operations have more use cases that come at the cost of setting up public cover identities for the operatives.

Clandestine and Covert Operations

Covert: A covert operation is an operation that is planned and executed in secrecy so that the identity of the agency or organization remains unknown or is plausibly deniable.

Clandestine: A clandestine operation is an operation that is carried out in such a manner that the operation remains in secrecy or is concealed.

Confusion of operative vs. organization in the application of privacy protection mechanisms from spy craft.

Exclusively clandestine measures are unsustainable for operative. Instead use covert measures to minimize the susceptibility of infrequent clandestine measures.

Use Covert to hide in plain sight.

Nest clandestine contexts inside covert contexts

Example:

Using a vpn on Saturday to trade on a Cyprus cryptocurrency exchange.

vs.

Using a vpn for all communications not merely the cryptocurrency exchange.

Communications context = herd privacy (covert)

Routing context = herd privacy (covert)

Interaction context (clandestine)

Analogy Clandestine vs Covert

The analogy for our purposes is that many approaches to internet privacy have looked like clandestine operations where the whole operation must be concealed and that concealment is largely technological.

But any leakage at all jeopardizes the whole operation.

This makes the approach fragile and largely unsustainable.

The ToIP TSP provides nested "tunneled" messaging contexts where the outer contexts can provide Covert herd privacy for the confidential inner contexts.


Strong
Privacy?
Weak
Weak

Strong Privacy

Definition: *uncorrelated* interactions over *unbounded* time and space.

Weak Privacy

Definition: *uncorrelated* interactions over *bounded* time and space.

Super aggregators and state actors are super correlators. They have effectively unlimited storage and computing capacity to *correlate* all digital *interactions*. Generative AIs are super correlators.

Eventually, all disclosed data will be correlated unless there is a strong enough incentive to decorrelate.

Decorrelation only occurs when the cost of correlation exceeds the value of correlation

Freedom

negative — balance — positive

Freedom from …	Freedom to …
exploitation (commercial)	extract value(commercial)
intimidation (social)	build relationships (social)
censorship (political)	build influence (political)

possibility of erasure = possibility of censorship

anonymity = loss of attributable value

untrackable = loss of enforceable value

Operating Regimes

Political	Economic: Illegitimate	Economic: Legitimate
Legitimate	Hide or Bribe	Hide, Regulate, or Legally Enforce Contracts *Stop hiding and start fighting back!*
Illegitimate	Hide and Bribe	Criminally Enforced Contracts?

Managing the Time Value of Information

In general, privacy dissipates over time. This is because digital information is inherently leaky, and those leaks become more correlatable as the body of leaks grows over time.

The primary exploitable time value of correlated information for data aggregators is that it can be used to predict behavior.

Advertisers want to predict who will most likely be receptive to their marketing campaigns.

The predictive accuracy of aggregated behavioral information of potential participants for any given market-related behavior is largely a function of the nearness in time of that market-related behavior when used to make the prediction.

We can ascribe a time constant to a given market for the exploitable predictive potential of market-related behavior where information older than the time constant no longer has net predictive value over the cost of aggregating it.

Information that exceeds this time constant is considered stale because there is no longer any incentive to aggregate and correlate it.

Therefore, even though privacy dissipates over time, the value of correlation also diminishes over time so that cost-effective privacy protection mechanisms can focus resources on near-term correlatability.

This provides a sweet spot for sustainable privacy protection governed by the time constant of the time value of exploitable correlation.

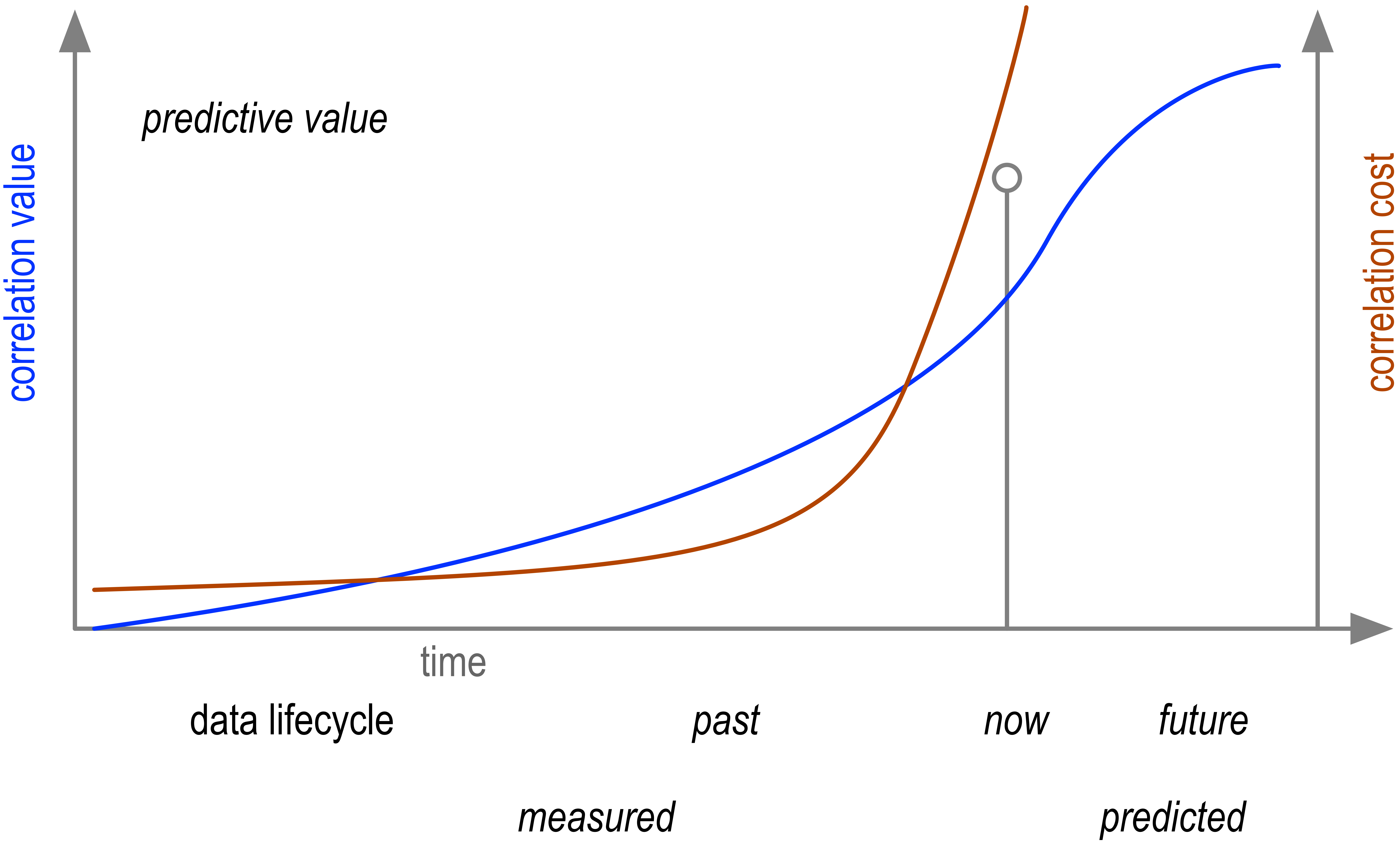
Likewise, the cost of privacy protection can be weighed against the cost due to the harm of exploitation.

If the cost of protection exceeds the cost due to the harm of exploitation, then it's not worth protecting (i.e., it's counterproductive to the protector).

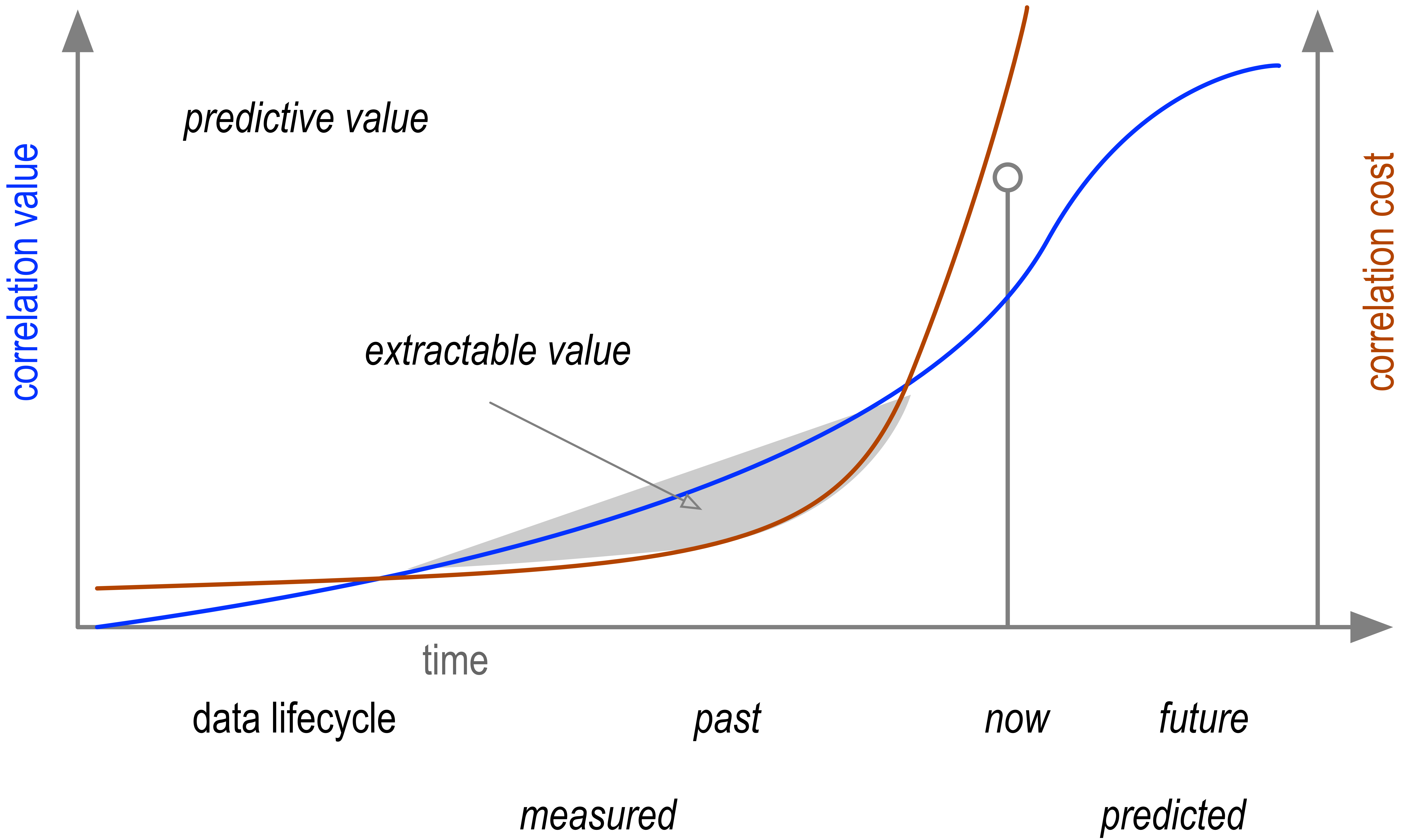
If the cost of correlation to exploit exceeds the time value return of exploitation, then it's not worth exploiting (i.e., it's counterproductive to the exploiter).

Therefore, the diminishing exploitable time value of correlated information can be used to balance the inherent leakiness of information.

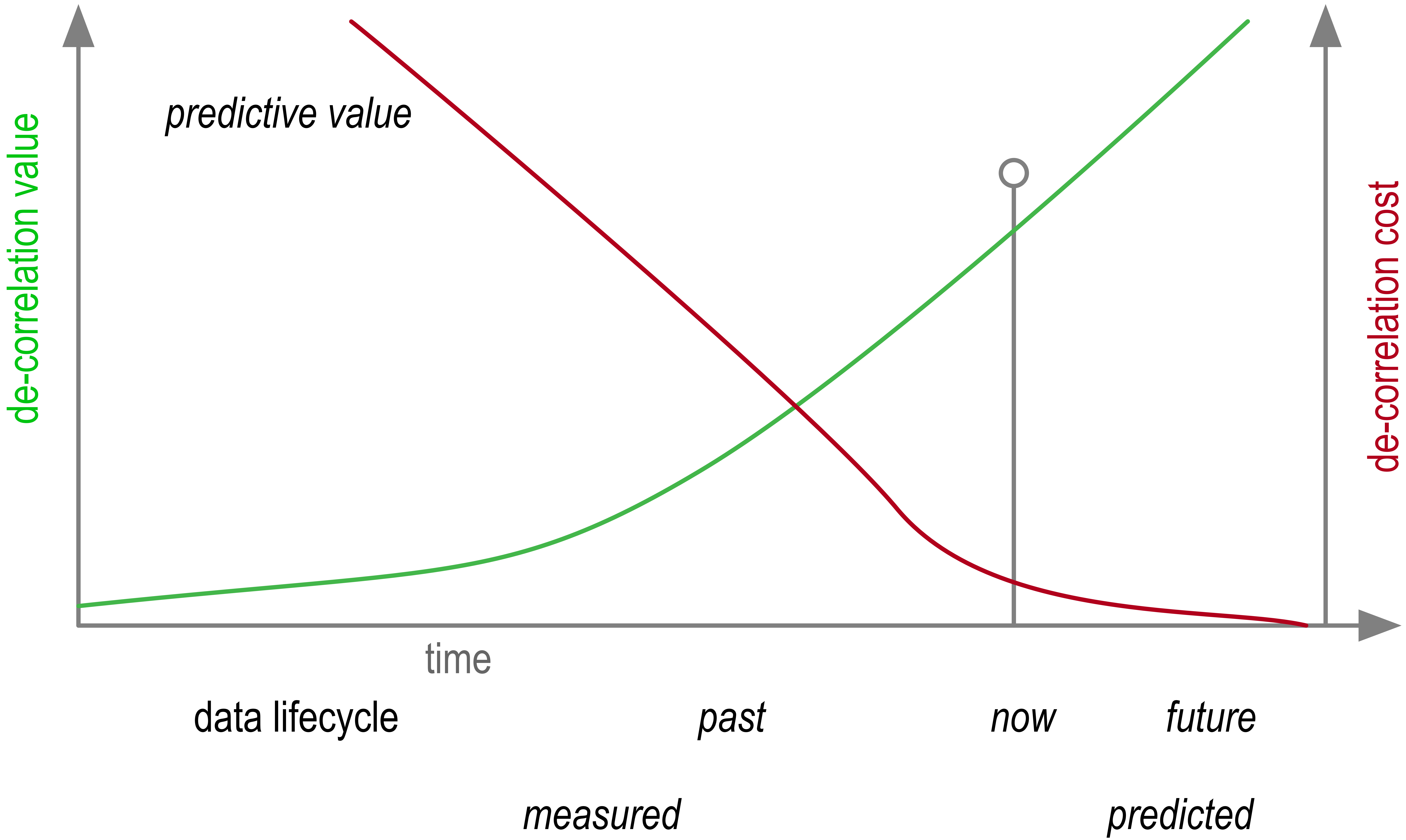
Economics of Correlator



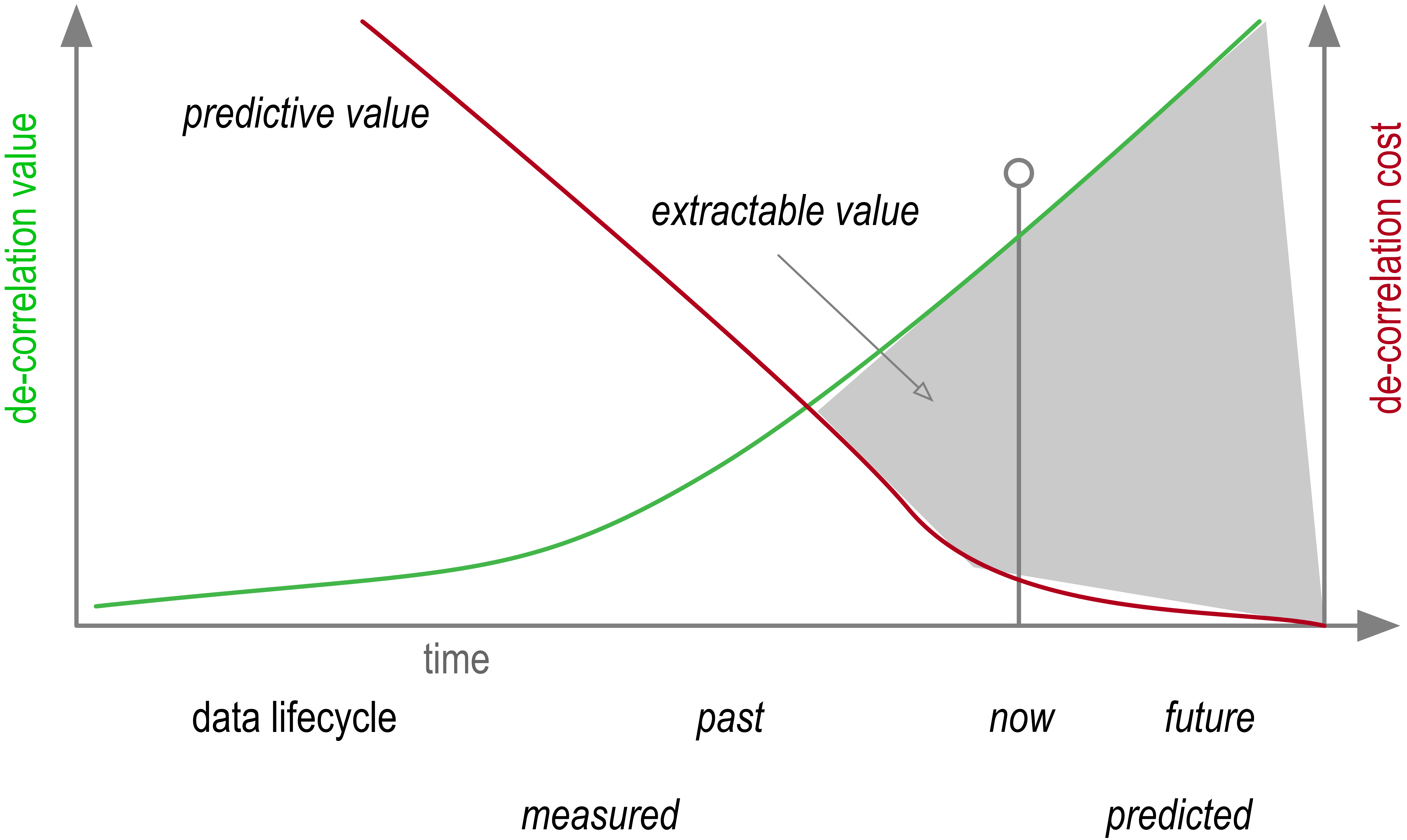
Economics of Correlator: Value Extraction



Economics of De-correlator



Economics of De-correlator: Value Extraction



User Public/Private Key Management: *Then* (< 2015) and *Now*

Then: impossibility of user-managed private keys

Result: federated identity: IDPs with PKI-DNS/CA, OAuth

Now: mobile devices/HSMs with MFA, secure boot/ enclaves, password management apps

Result: practical user-managed private keys

Then: *good enough* security from federated identity

Result: session security, perimeter security, weak auth-crypt for AuthN

Now: identity based on user-managed private key(s)

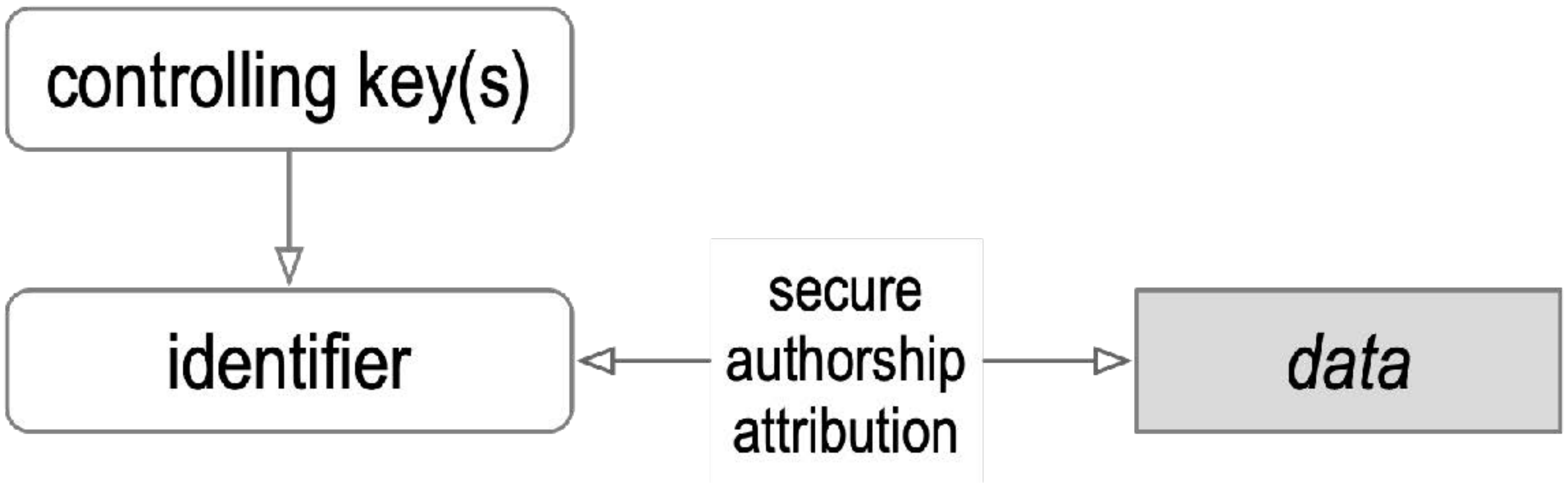
Result: KERI

First Principles Approach to the Universal Secure Attribution Problem

Establish authorship of data, documents, credentials, entitlements, …

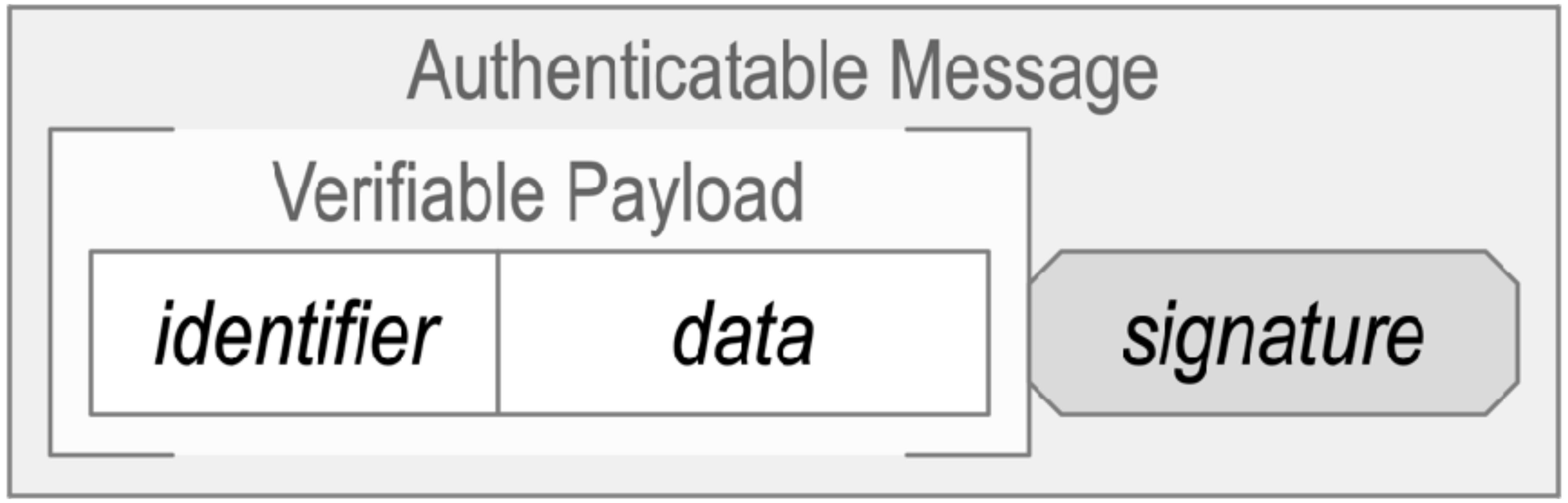
- Authentic data provenance by anyone to anyone from anyone, i.e. *universal*
- Cryptographically verifiable, non-repudiable secure attribution of any communication to its source

Solve authentic data provenance via universal secure attribution



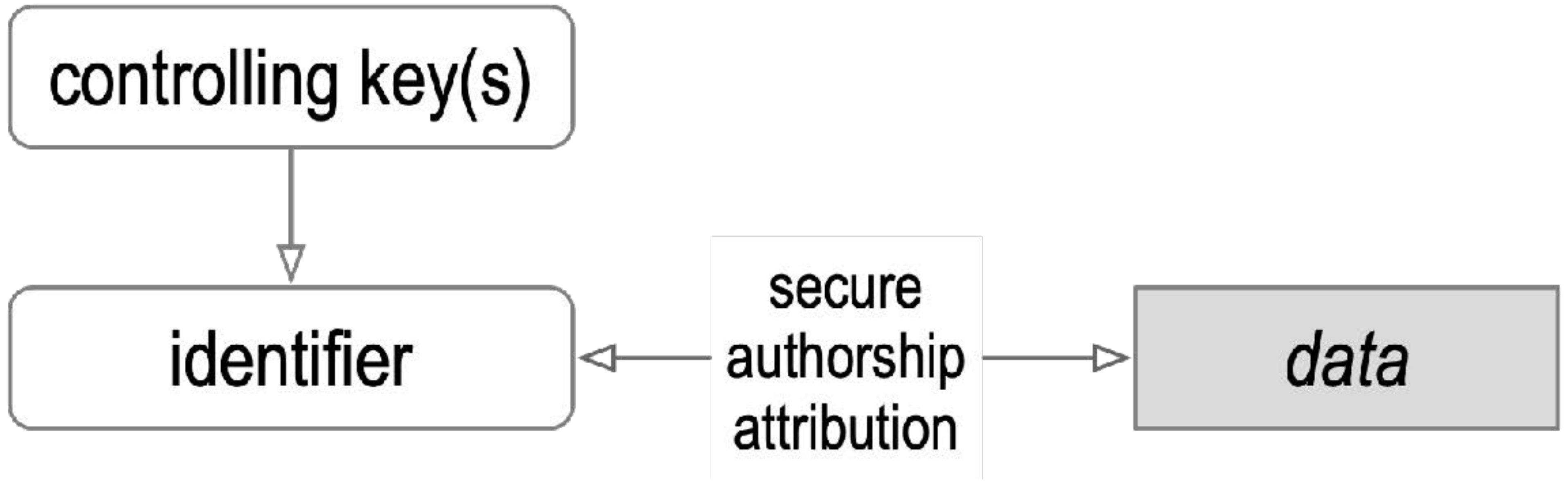
Identity (-ifier) System Security Overlay

Establish authenticity (securely attribute source) of message payload.



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

Private Key Management



The continued use of private keys *exposes* them to *side-channel* attacks.

This exposure *weakens* private keys over time (as the likelihood of a successful attack rises).

Thus, from time to time, private keys must be revoked and replaced, i.e., rotated

Conventional PKI must re-establish the root-of-trust with each rotation

Thereby making rotation highly vulnerable to attack

Compromised private keys result in loss of control over the identifier

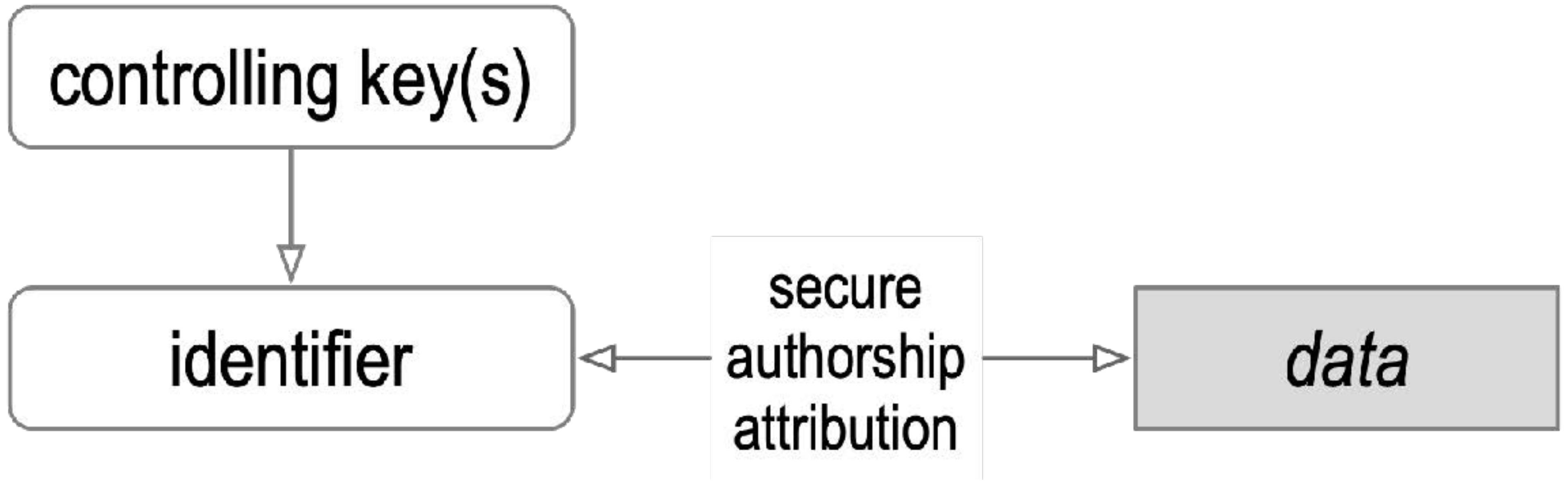
This breaks the chain-of-trust-of-control over the identifier

Key compromise recovery must detect and regain control over the identifier

Key rotation with key compromise recovery is the *hard problem* of private key management

KERI solves this hard problem

Identifier Theory

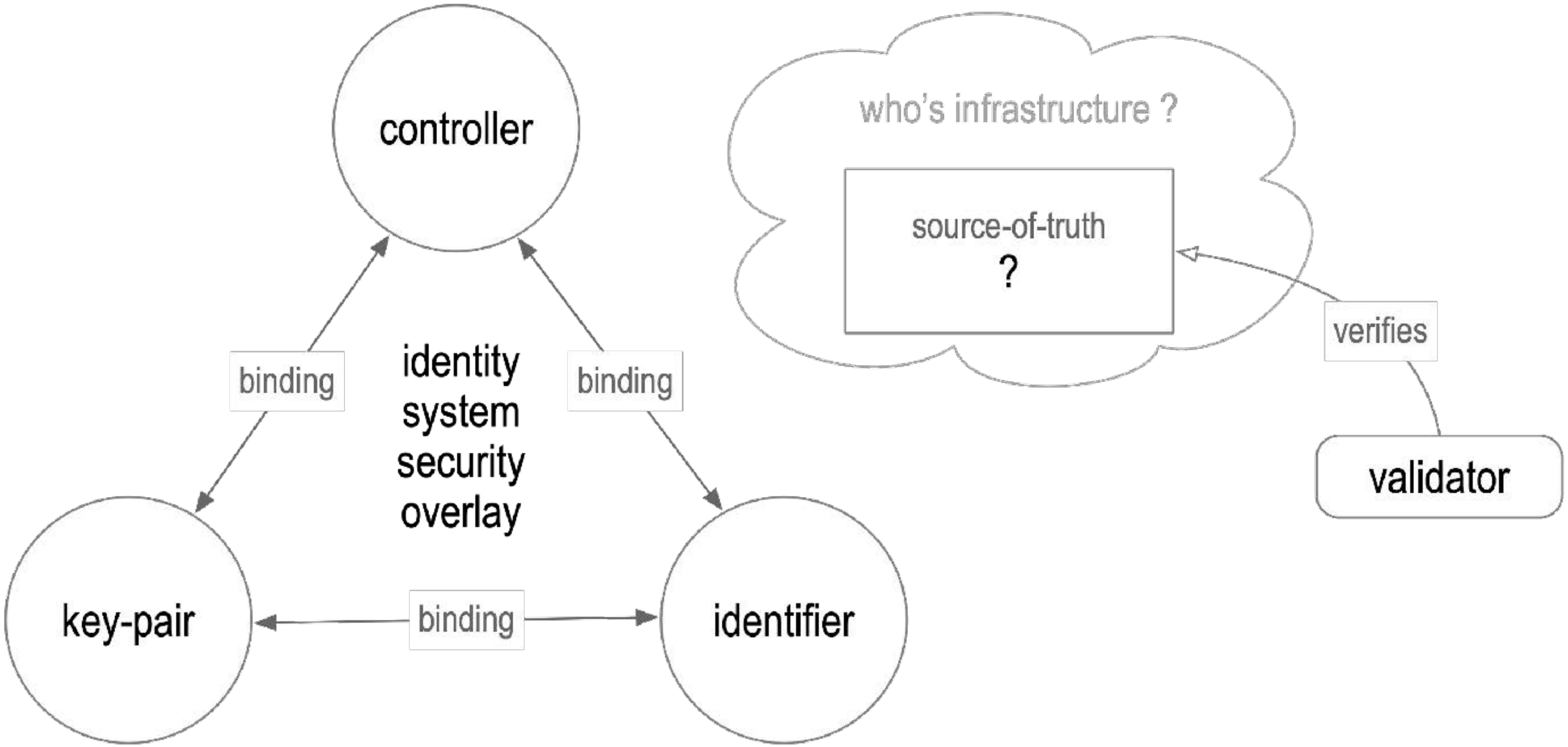


Short-term key-pair with public key as identifier = ephemeral identifier
Long-term key-pair with public key as identifier = less ephemeral identifier
Cryptographically derived identifier controlled by rotatable key-pair(s) = persistent (unbounded-term) identifier

Trust Basis of a Trust Domain

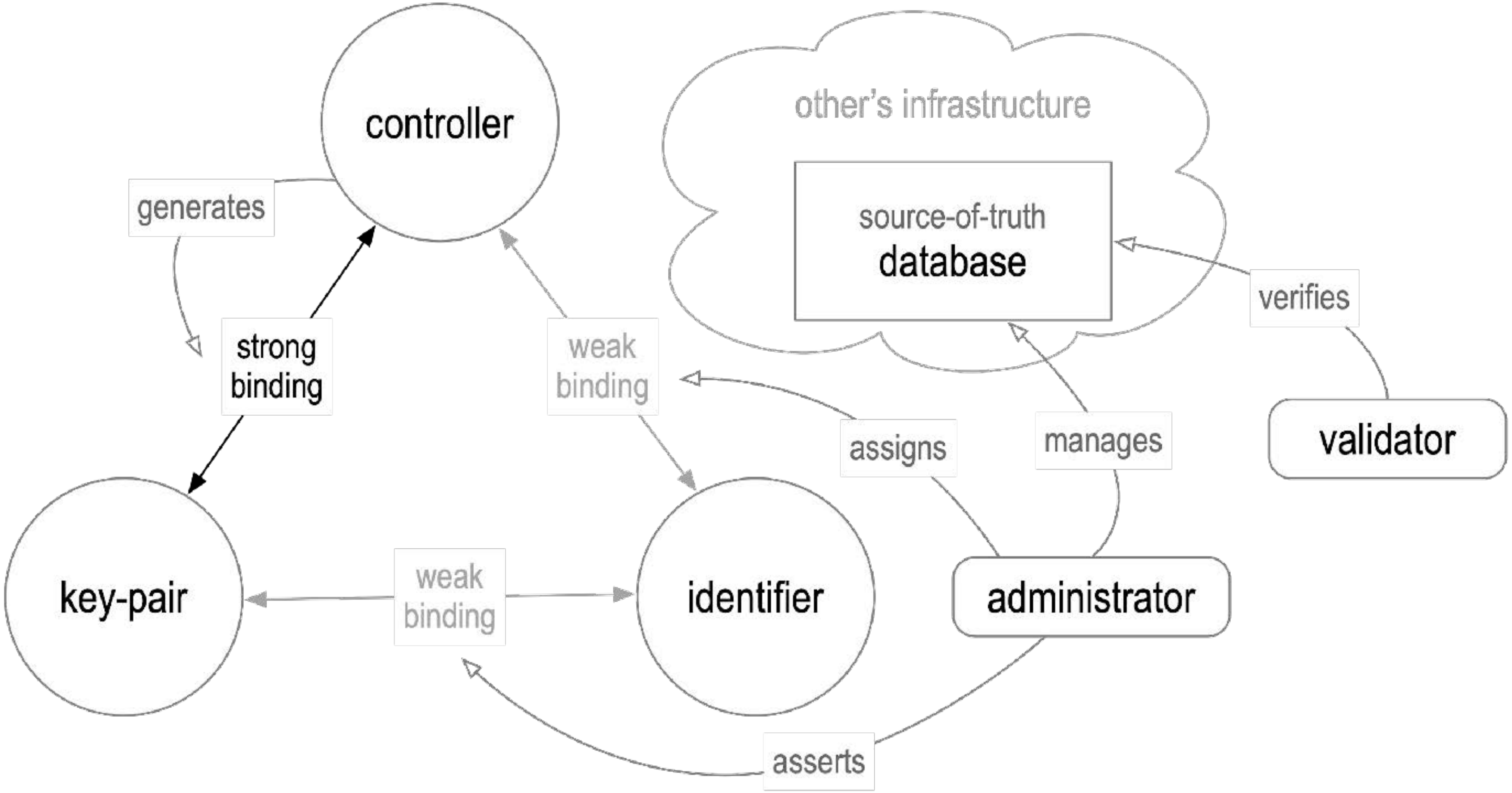
A *trust basis* binds controllers, identifiers, and key-pairs.

A *trust domain* is the ecosystem of interactions (functions) that rely on a trust basis.



Administrative Trust Basis

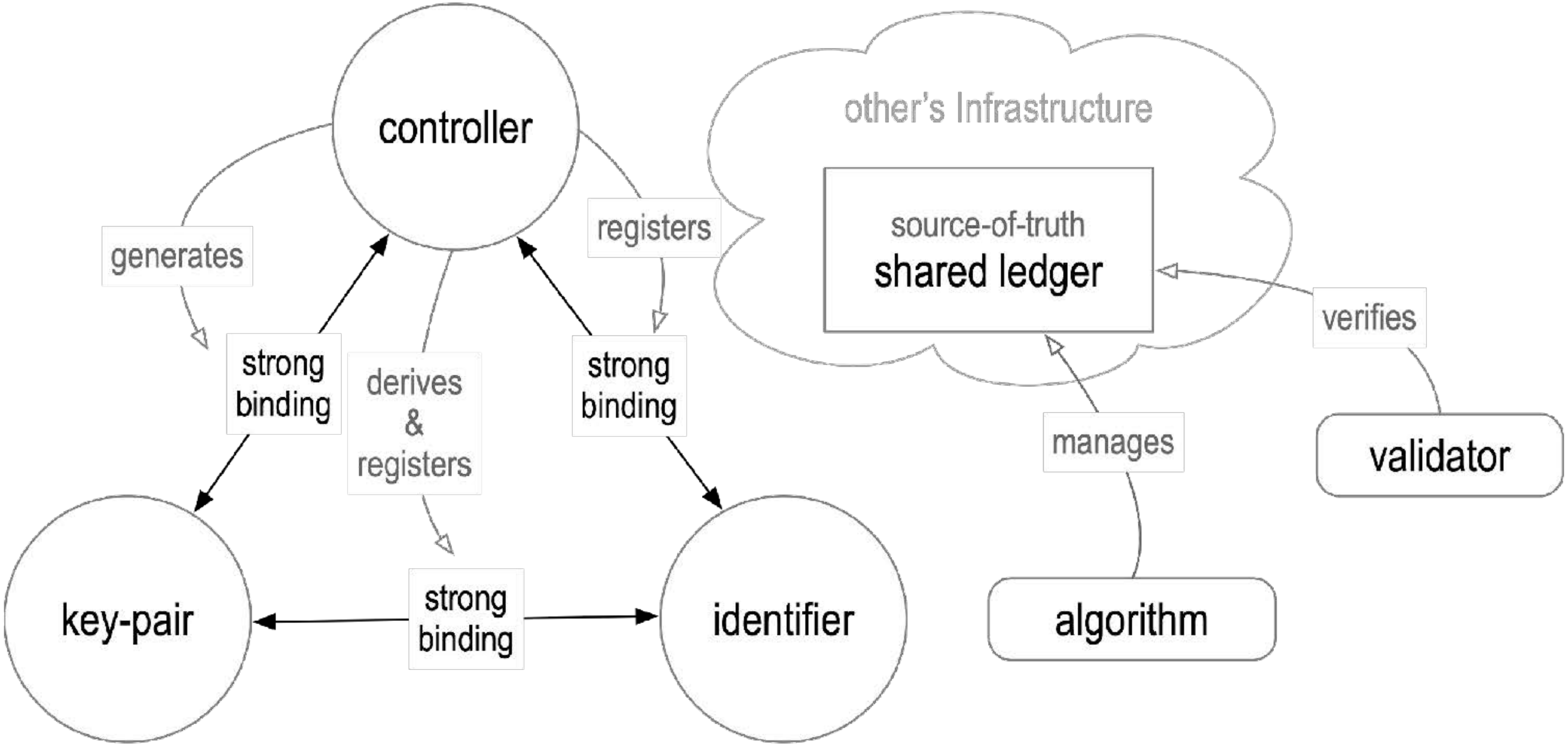
DNS/CA, OIDC IP



root-of-trust in non-verifiable operational infrastructure with opaque governance

Algorithmic Trust Basis

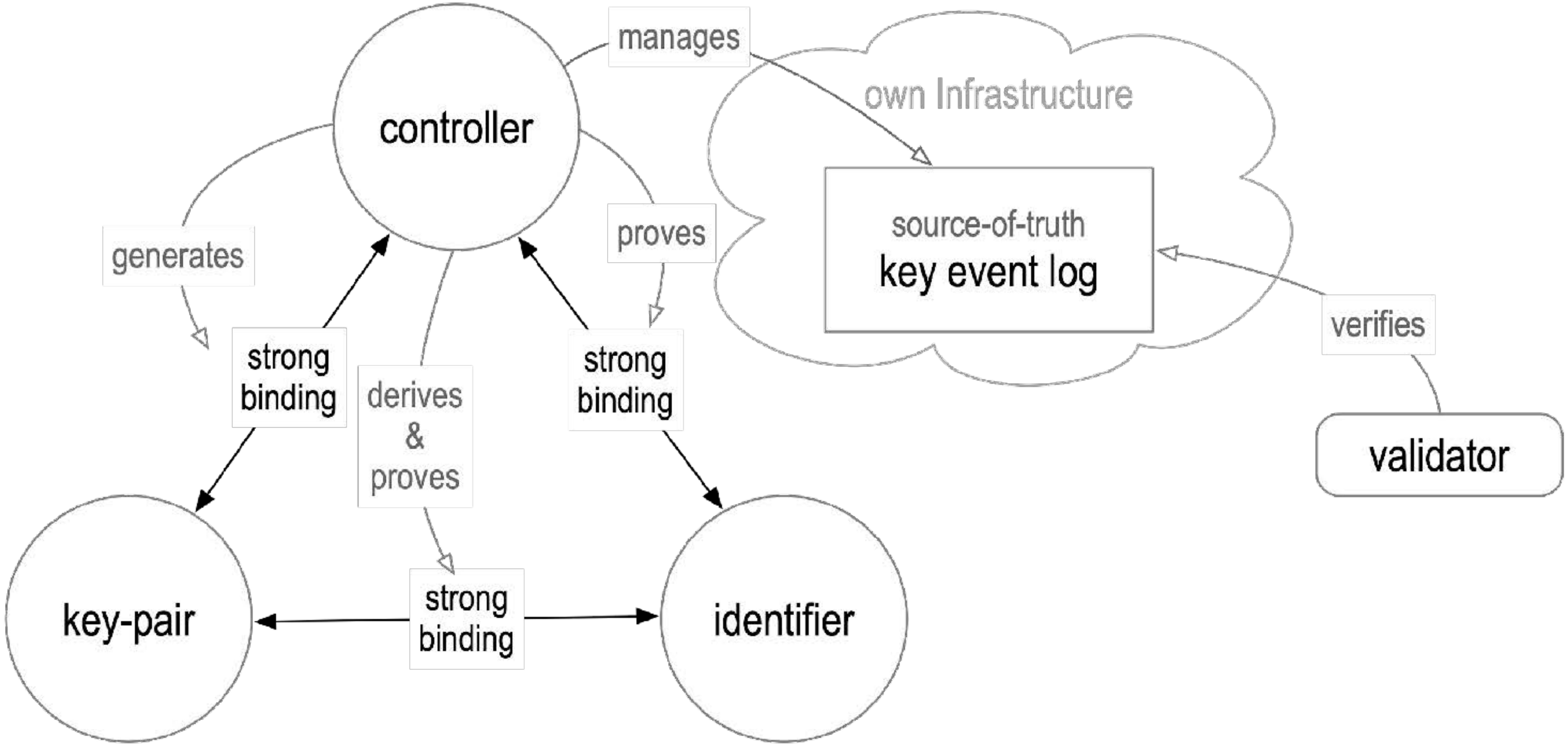
Shared distributed ledgers



root-of-trust in verifiable operational infrastructure with shared governance

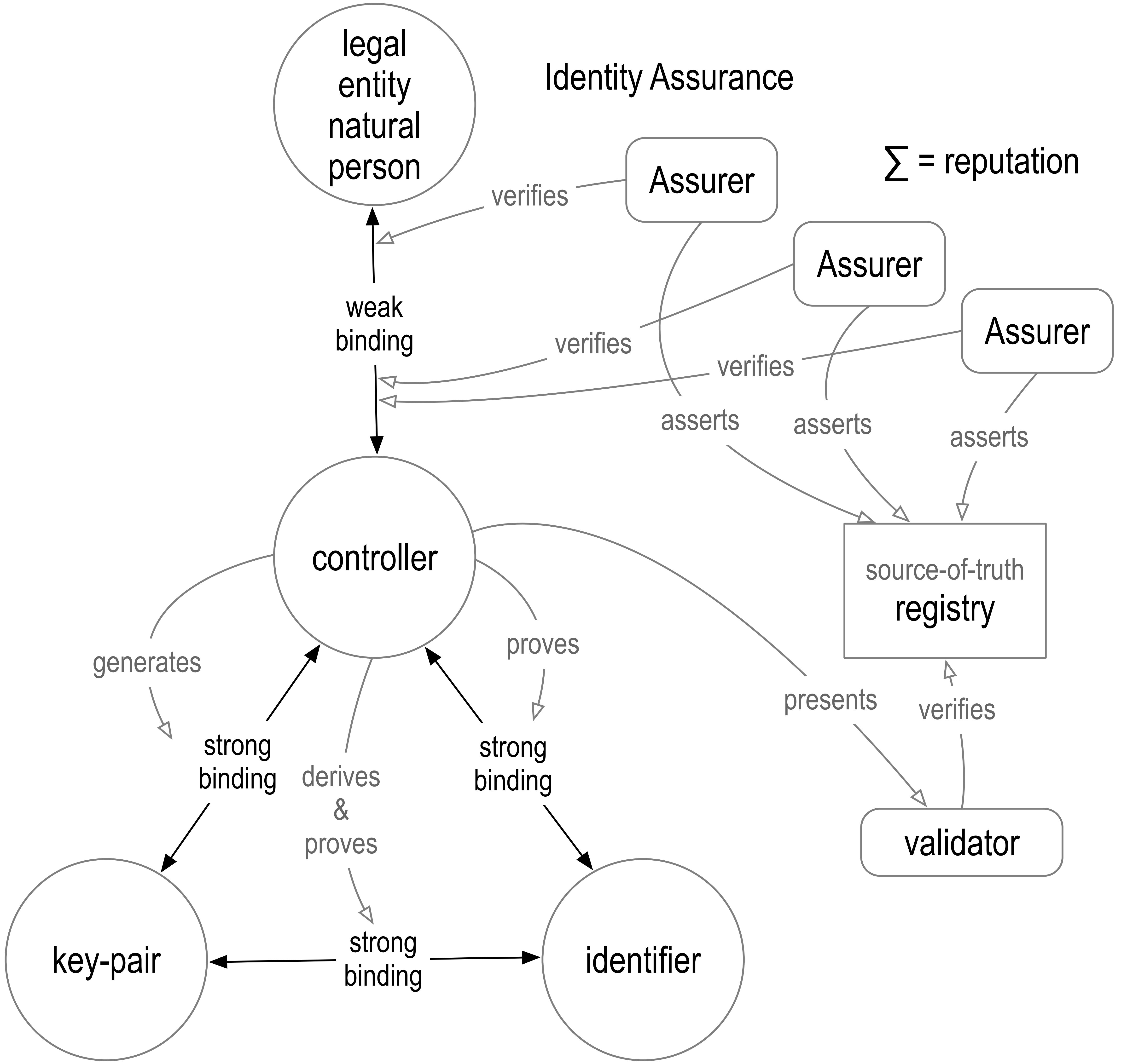
Autonomic Trust Basis

Cryptographic proofs via verifiable data structures



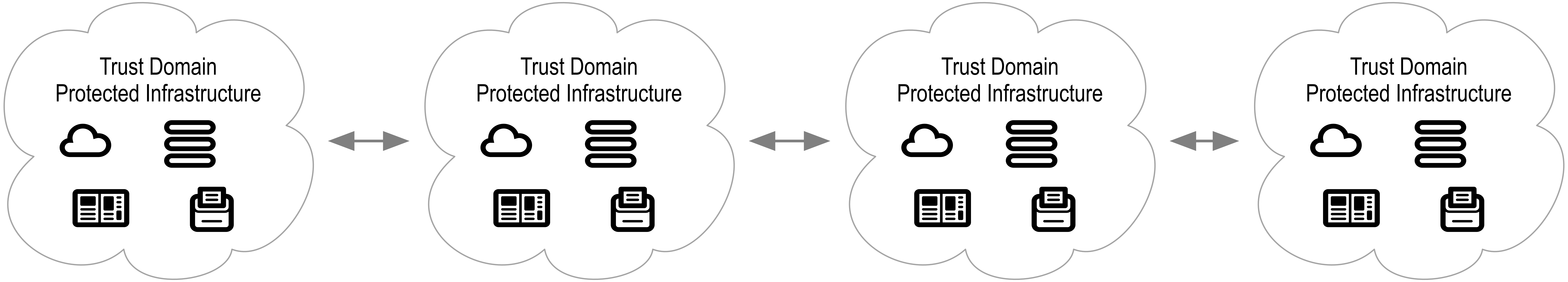
root-of-trust in verifiable cryptographic proofs of infrastructure with no shared governance

Identity Assurance and Reputation



Relatively weak binding reinforced by multiple bindings = reputation

Autonomic Trust Basis Enables Solving the Hard Problem of Moving Data Across Trust-Domains



Globally portable, at-scale

No identity theft (fraud-free cross-domain)

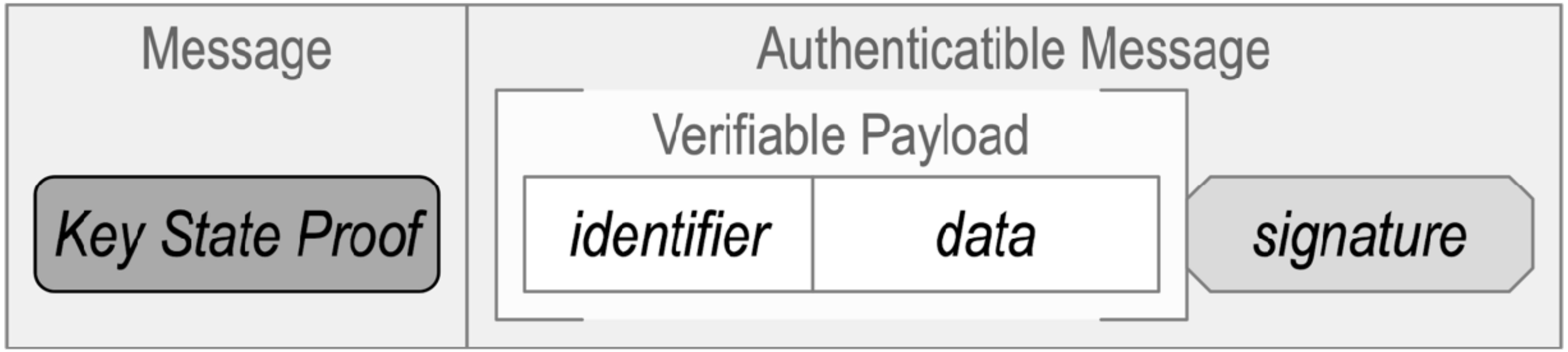
No shared secrets as primary authenticators

- no passwords
- no DH encryption keys
- no bearer tokens
- no PII

Identity (-ifier) System Security Overlay

persistent mapping via verifiable data structure of key state changes

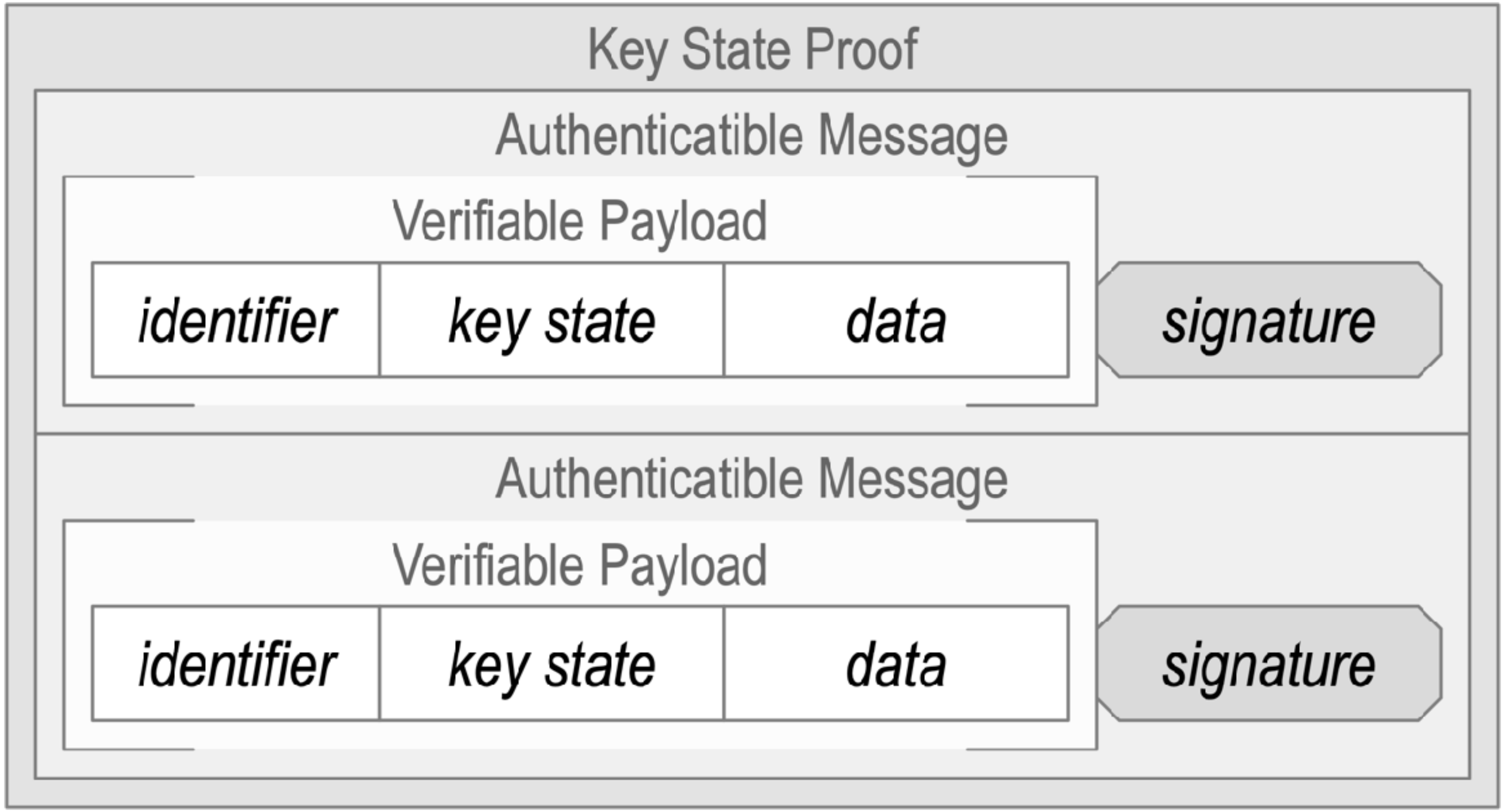
Establish authenticity (securely attribute source) of the message payload



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

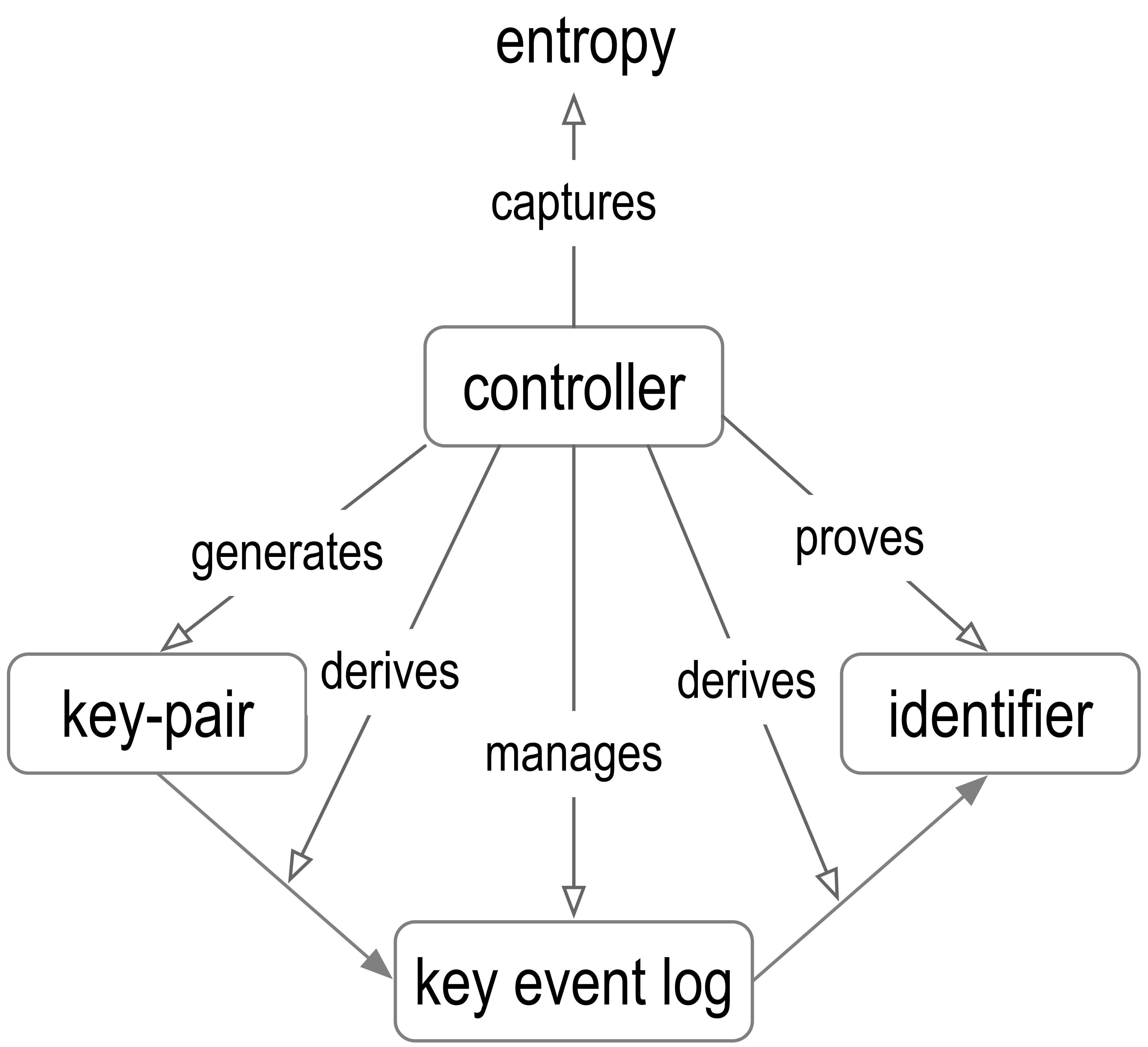
Key State Proof is Recursive Application of Overlay

Persistent mapping via a verifiable data structure of key state changes

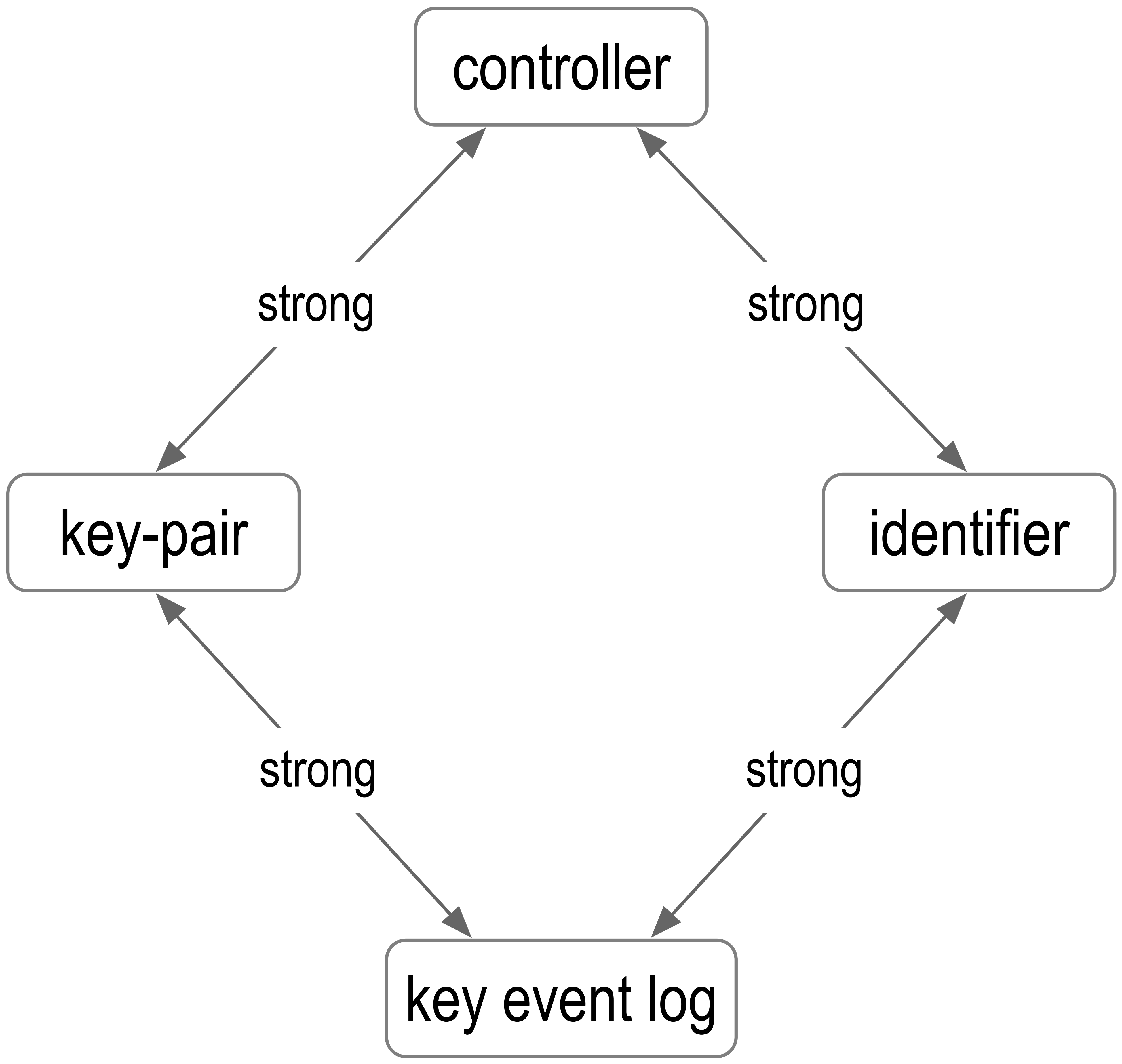


universally verifiable duplicity evident append-only backward and forward-chained key event log

Autonomic Identifiers (AIDs): Issuance and Binding
How to construct a cryptographic root-of-trust



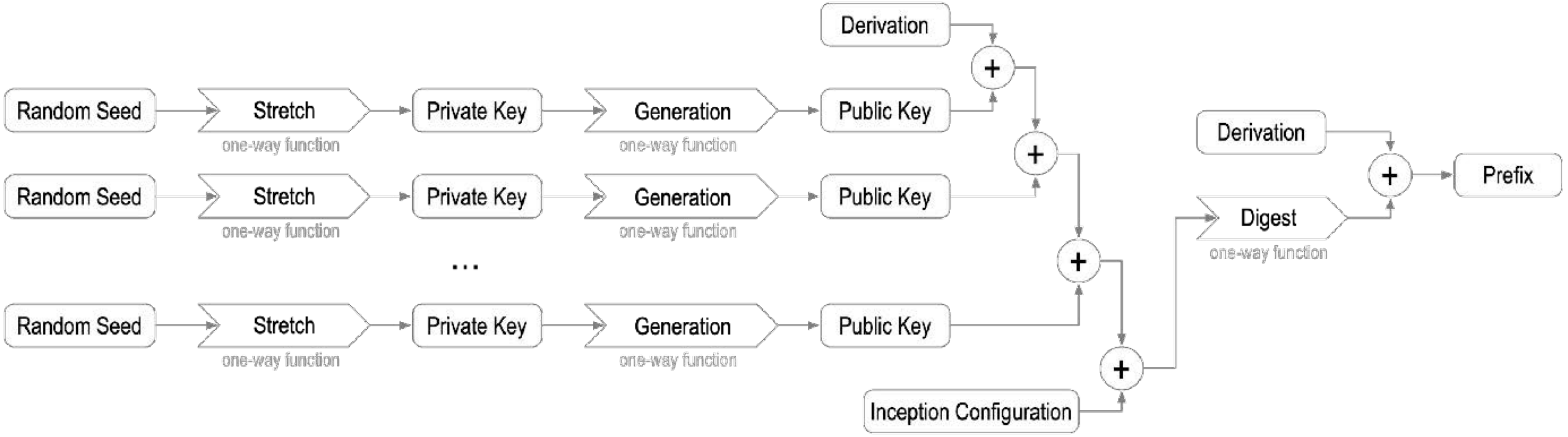
autonomic, self-managing

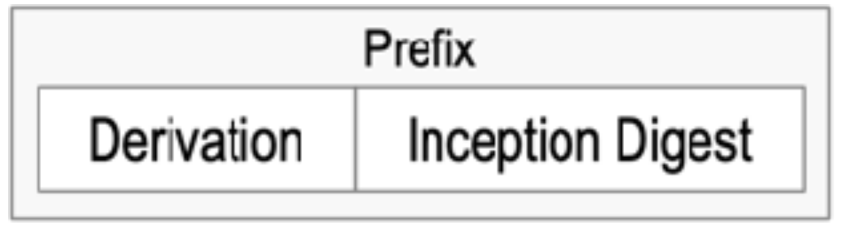


autonomic identifier binding tetrad

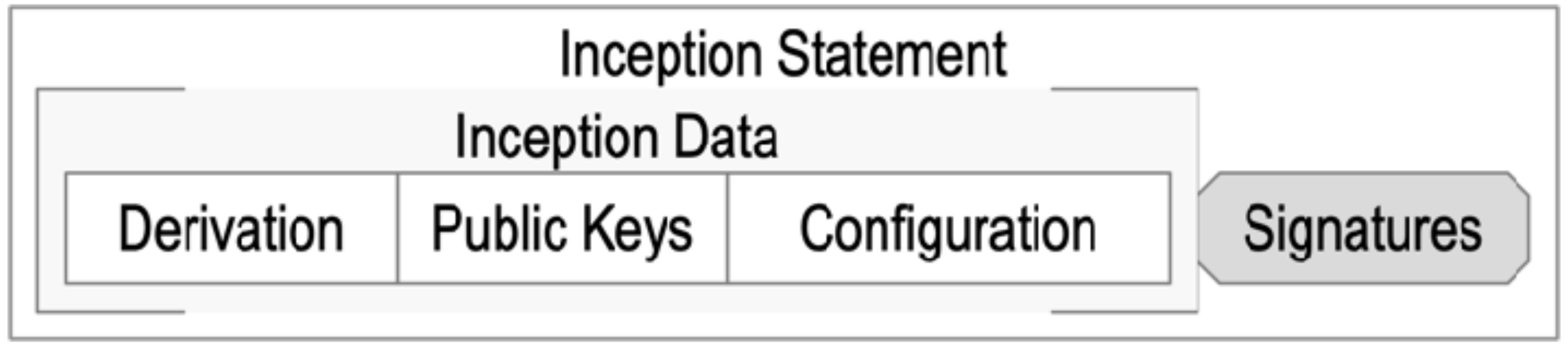
cryptographic root-of-trust with verifiable persistent control over the AID

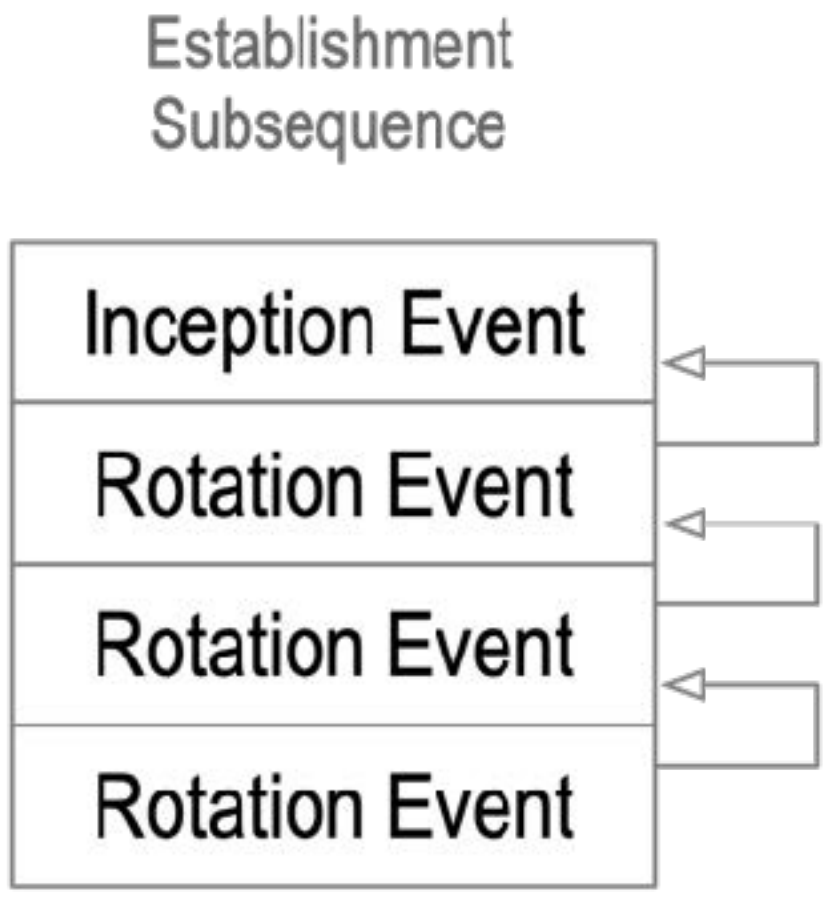
Cryptographic Root-of-Trust: Autonomic Identifier (AID)





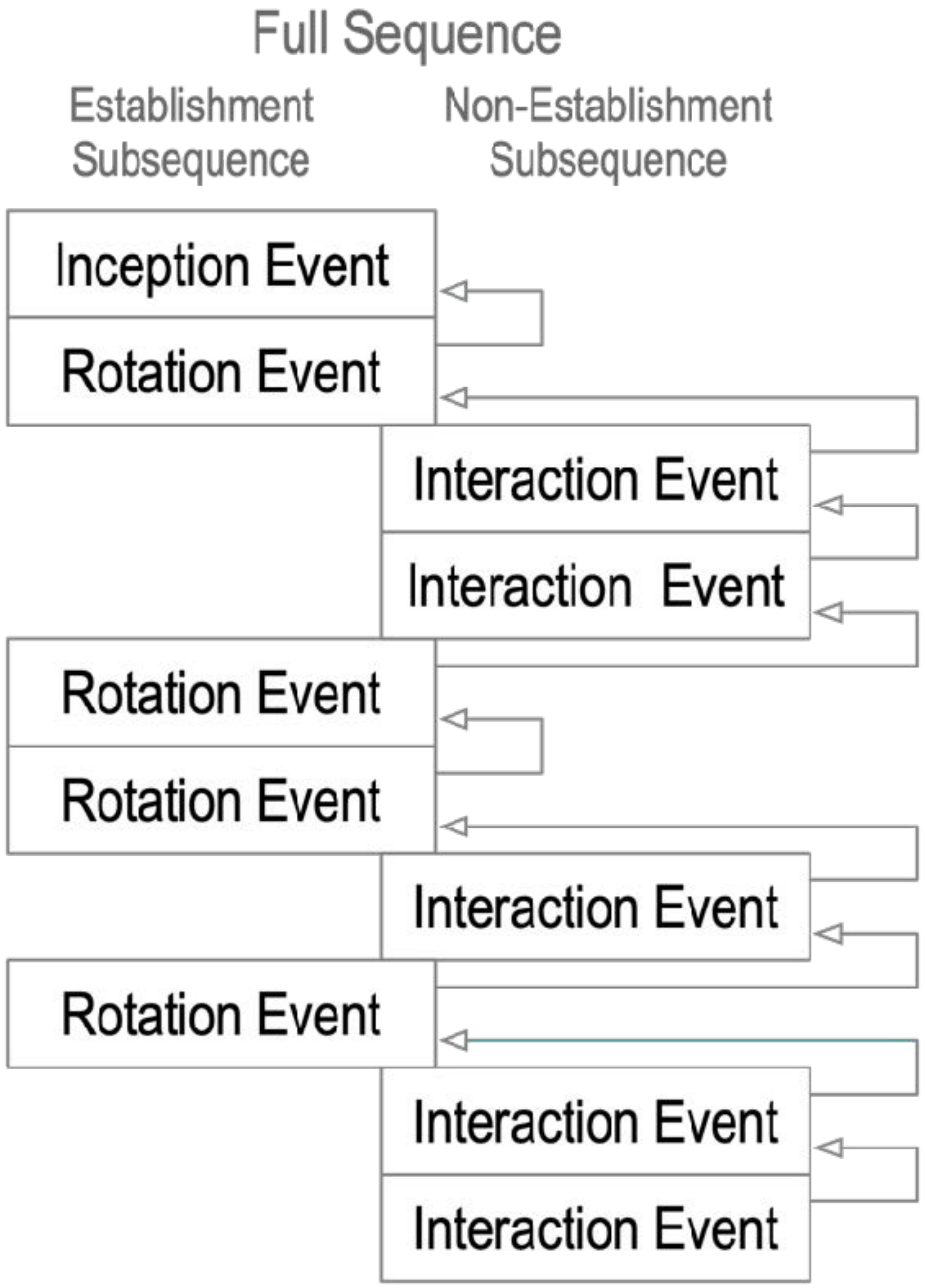
Key Event Log



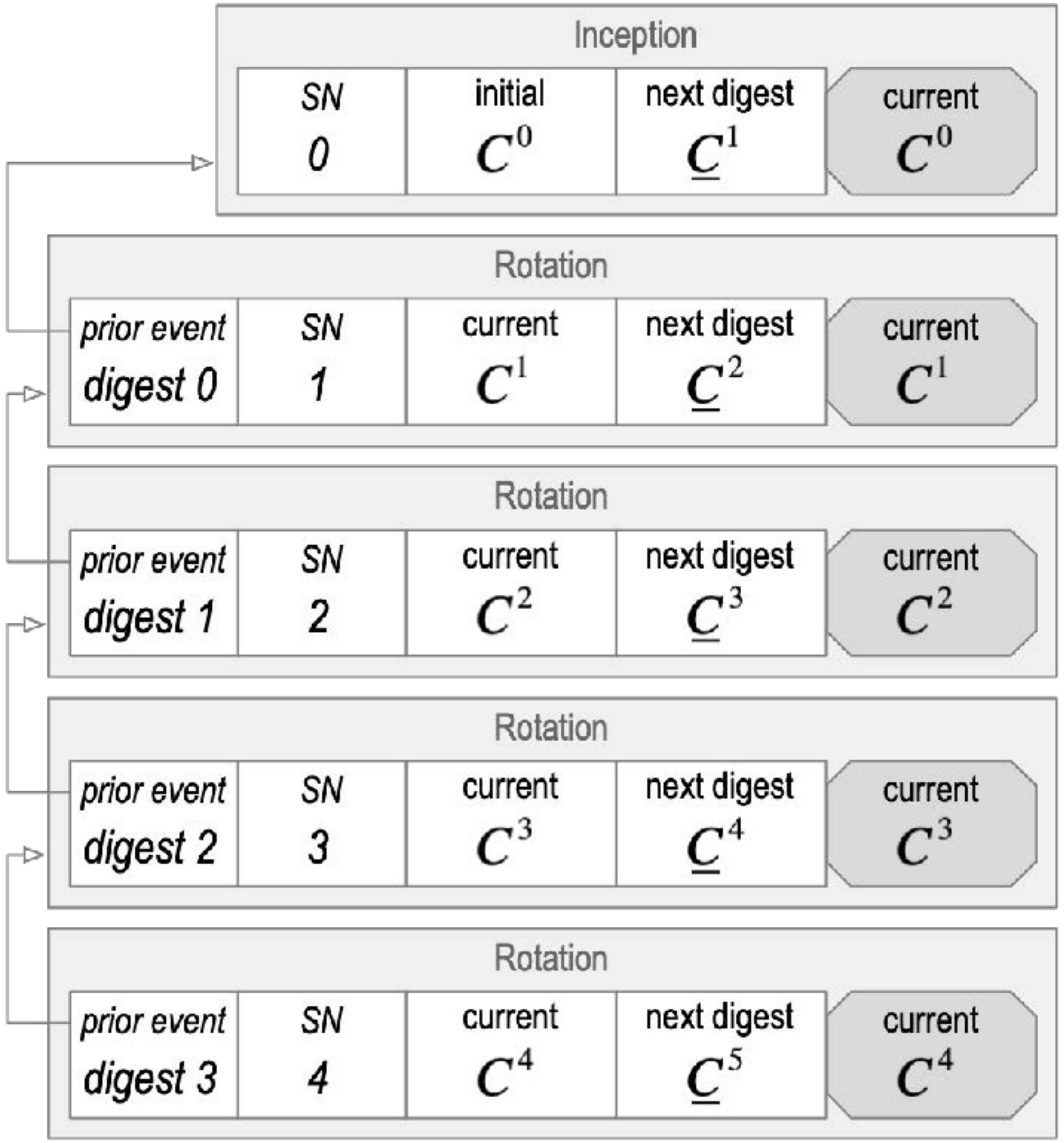


EL0JRaU2_RxFP0AL43wYn148Xq5YqaL6L48pf0fu7IUh

Key Pre-Rotation



KEL = duplicity evident verifiable data structure



Crypto-agility with pre-rotated digest(s) of *next* key(s) enable recovery from a surprise quantum attack

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

Inception Event

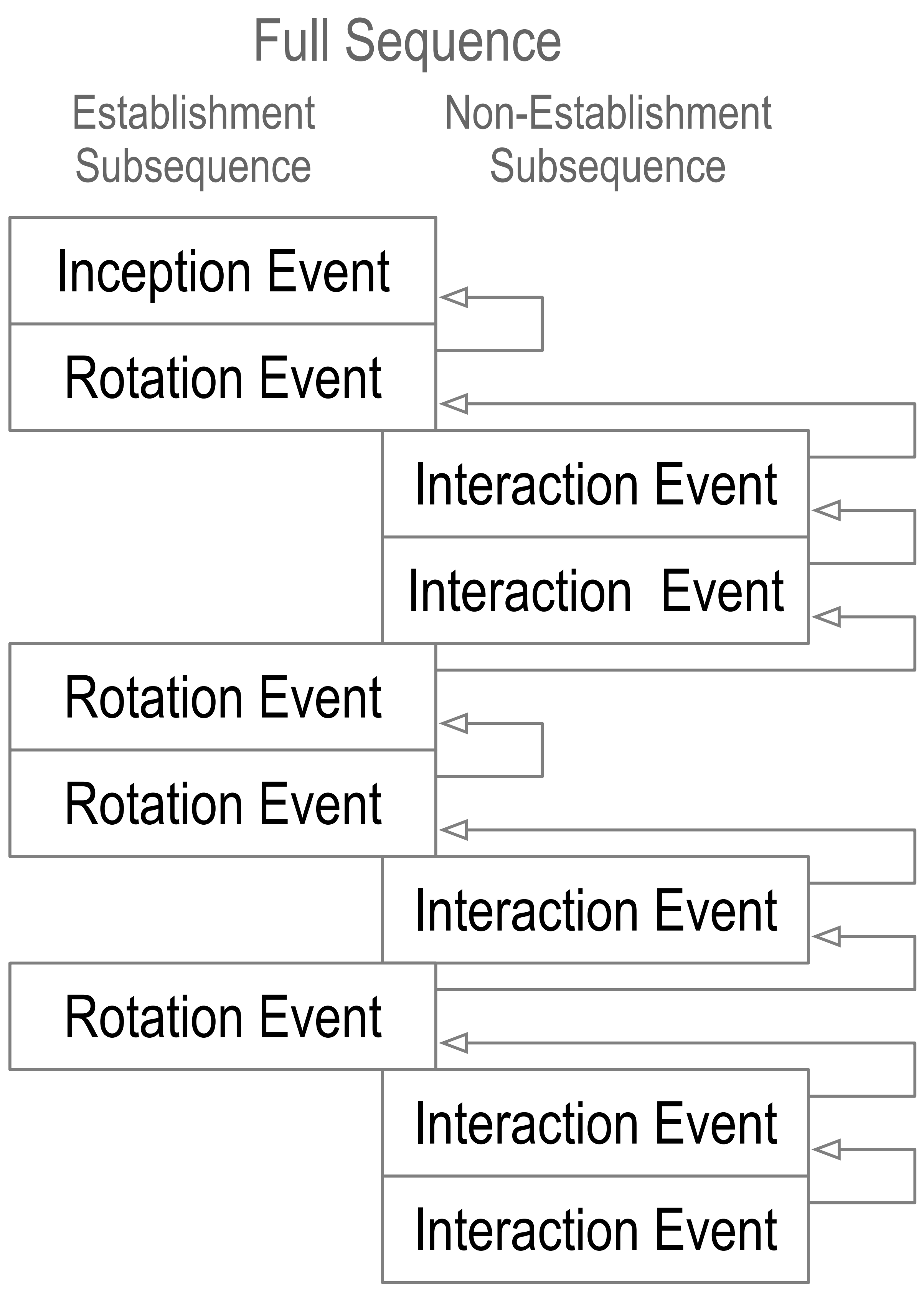
JSON

```json
{
    "v": "KERICAACAAJSONAAKp.",
    "t": "icp",
    "d": "EPR7FWsN3tOM8PqfMap2FRfF4MFQ4v3ZXjBUcMVtvhmB",
    "i": "EPR7FWsN3tOM8PqfMap2FRfF4MFQ4v3ZXjBUcMVtvhmB",
    "s": "0",
    "kt": "2",
    "k":
    [
        "DBFiIgoCOpJ_zW_OO0GdffhHfEvJWb1HxpDx95bFvufu",
        "DG-YwInLUxzVDD5z8SqZmS2FppXSB-ZX_f2bJC_ZnsM5",
        "DGIAk2jkC3xuLIe-DI9rcA0naevtZiKuU9wz91L_qBAV"
    ],
    "nt": "2",
    "n":
    [
        "ELeFYMmuJb0hevKjhv97joA5bTfuA8E697cMzi8eoaZB",
        "ENY9GYShOjeh7qZUpIipKRHgrWcoR2WkJ7Wgj4wZx1YT",
        "EGyJ7y3TlewCW97dgBN-4pckhCqsni-zHNZ_G8zVerPG"
    ],
    "bt": "3",
    "b":
    [
        "BGKV6v93ue5L5wsgk75t6j8TcdgABMN9x-eIyPi96J3B",
        "BJfueFAYc7N_V-zmDEn2SPCoVFx3H20alWsNZKgsS1vt",
        "BAPv2MnoiCsgOnklmFyfU07QDK_93NeH9iKfOy8V22aH",
        "BA4PSatfQMw1lYhQoZkSSvOCrE0Sdw1hmmniDL-yDtrB"
    ],
    "c": ["DID"],
    "a": []
}
```

CESR

```
-FCS # Key Event Counter FixBodyGroup count=146 quadlets
  0OKERICAACAA # 'v' version  Verser Tag10 proto=KERI vrsn=2.00
  Xicp # 't' message type Ilker Tag3 Ilk=icp
  EDZOA3y_b_0LG4_cfpKTbWU-_3eeYNM0w9iTkT7frTYs # 'd' SAID Diger Blake3_256
  EDZOA3y_b_0LG4_cfpKTbWU-_3eeYNM0w9iTkT7frTYs # 'i' AID Prefixer Blake3_256
  MAAA # 's' Number Short sn=0
  MAAC # 'kt' Tholder signing threshold=2
  -JAh # 'k' Signing Key List Counter GenericListGroup count=33 quadlets
    DBFiIgoCOpJ_zW_OO0GdffhHfEvJWb1HxpDx95bFvufu # key Verfer Ed25519
    DG-YwInLUxzVDD5z8SqZmS2FppXSB-ZX_f2bJC_ZnsM5 # key Verfer Ed25519
    DGIAk2jkC3xuLIe-DI9rcA0naevtZiKuU9wz91L_qBAV # key Verfer Ed25519
  MAAC # 'nt' Tholder rotation threshold=2
  -JAh # 'n' Rotation Key Digest List Counter GenericListGroup count=33 quadlets
    ELeFYMmuJb0hevKjhv97joA5bTfuA8E697cMzi8eoaZB # key digest Diger Blake3_256
    ENY9GYShOjeh7qZUpIipKRHgrWcoR2WkJ7Wgj4wZx1YT # key digest Diger Blake3_256
    EGyJ7y3TlewCW97dgBN-4pckhCqsni-zHNZ_G8zVerPG # key digest Diger Blake3_256
  MAAD # 'bt' Tholder Backer (witness) threshold=3
  -JAs # 'b' Backer (witness)List Counter GenericListGroup count=44 quadlets
    BGKV6v93ue5L5wsgk75t6j8TcdgABMN9x-eIyPi96J3B # AID Prefixer Ed25519N
    BJfueFAYc7N_V-zmDEn2SPCoVFx3H20alWsNZKgsS1vt # AID Prefixer Ed25519N
    BAPv2MnoiCsgOnklmFyfU07QDK_93NeH9iKfOy8V22aH # AID Prefixer Ed25519N
    BA4PSatfQMw1lYhQoZkSSvOCrE0Sdw1hmmniDL-yDtrB # AID Prefixer Ed25519N
  -JAB # 'c' Config Trait List Counter GenericListGroup count=1 quadlets
    XDID # trait Traitor Tag3 trait=DID
  -JAA # 'a' Seal List Counter GenericListGroup count=0 quadlets
```

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 a self-certifying cryptographic root-of-trust protects against internal inconsistency.

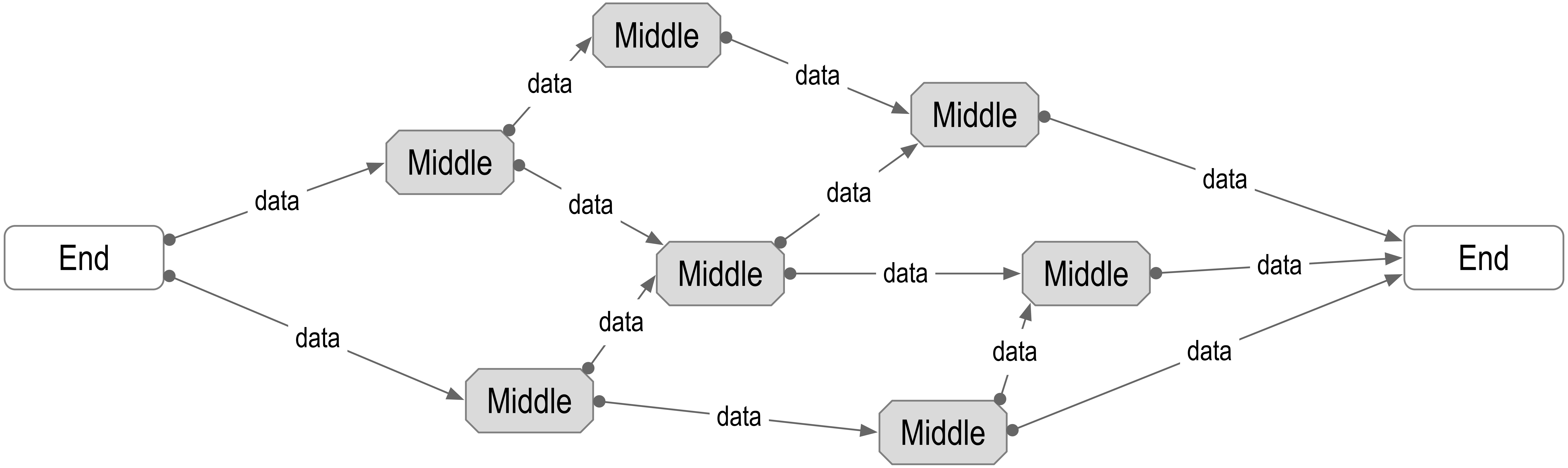
Externally inconsistent logs. Two different logs for the same identifier, both verifiable = duplicity.

Duplicity detection protects against external inconsistency.

KERI provides duplicity evident DKMI

End Verifiability

End-to-End Verifiability   *Authenticity*

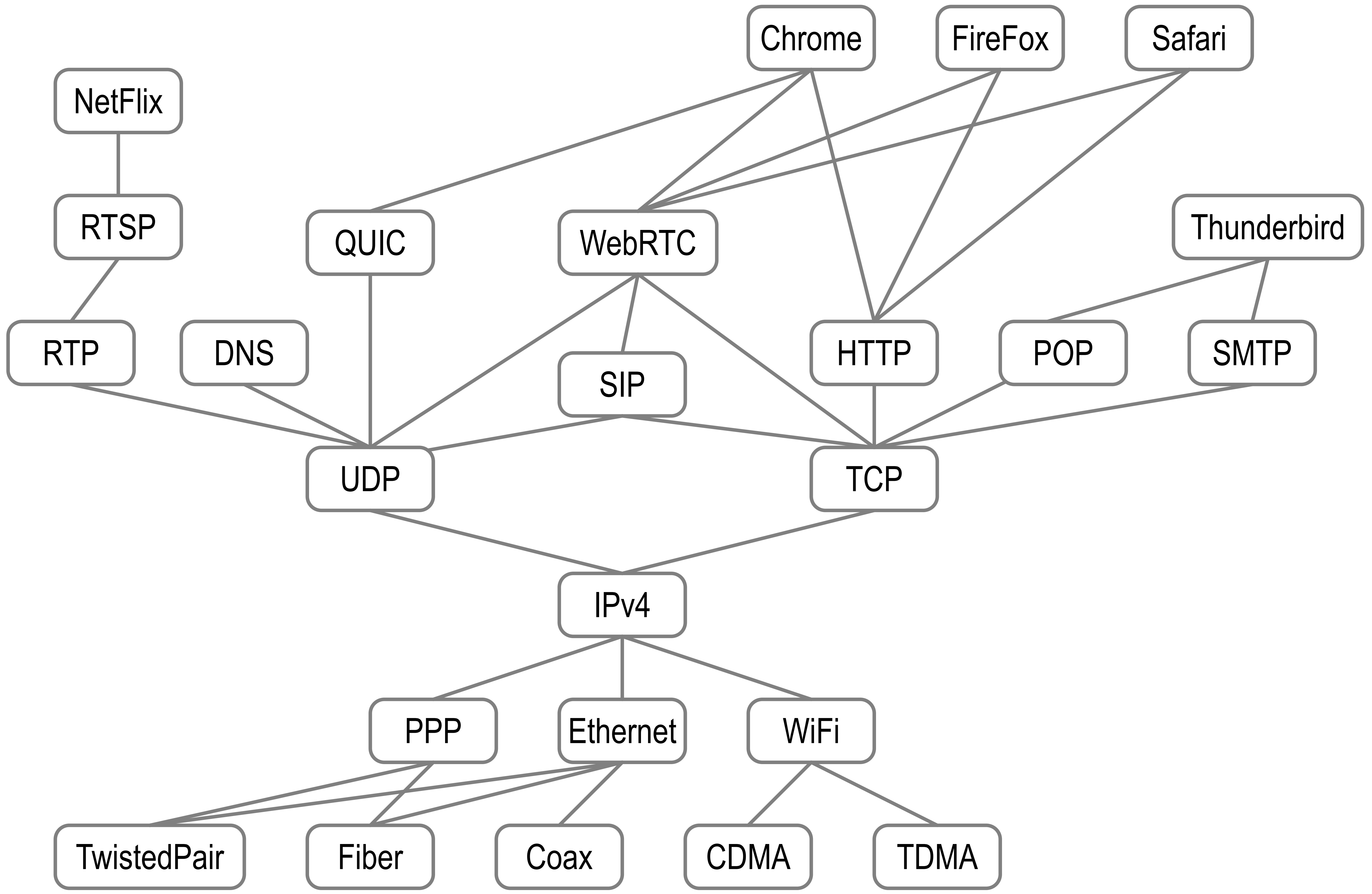


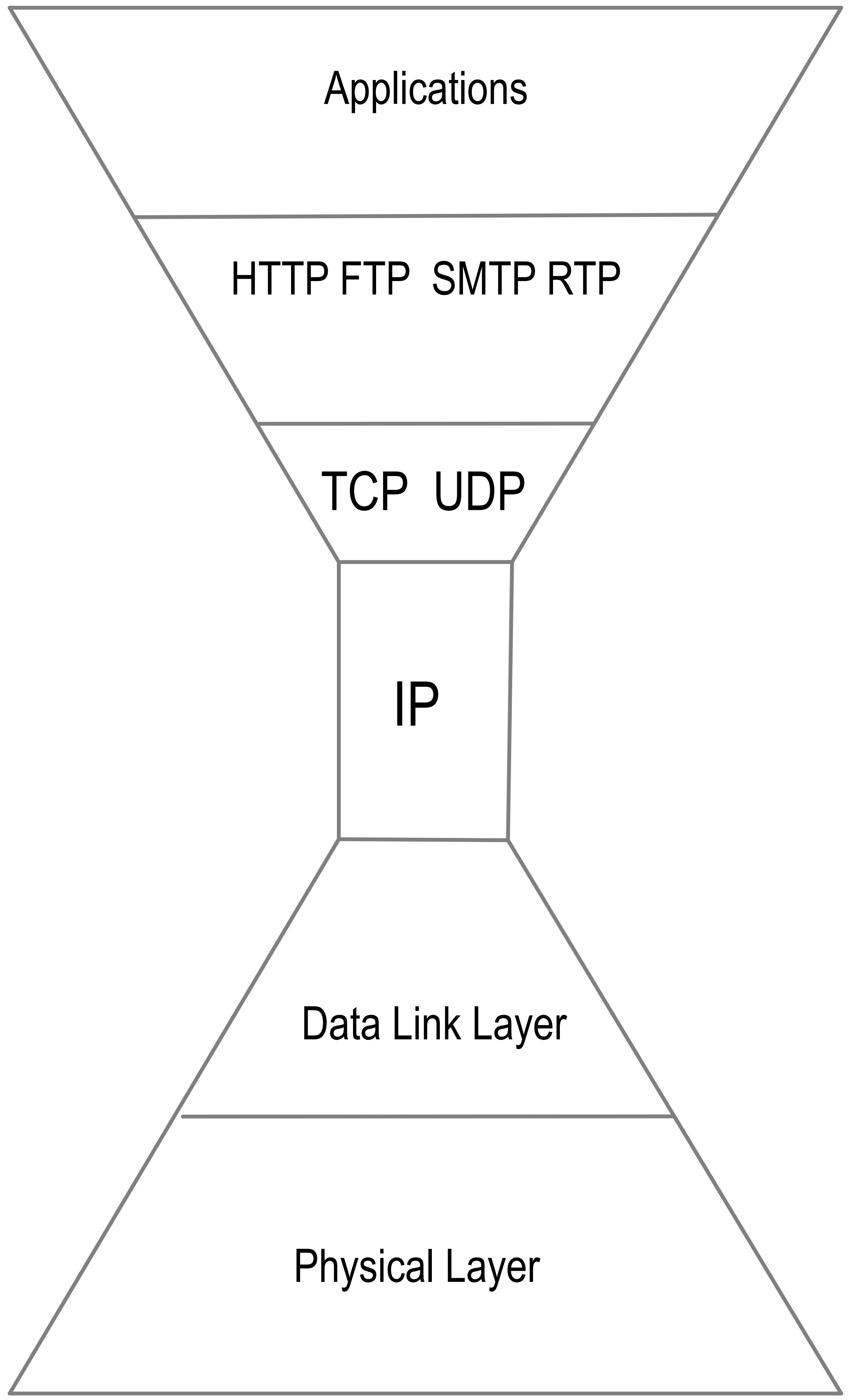
Its much easier to protect one's private keys than to protect all internet infrastructure

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

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

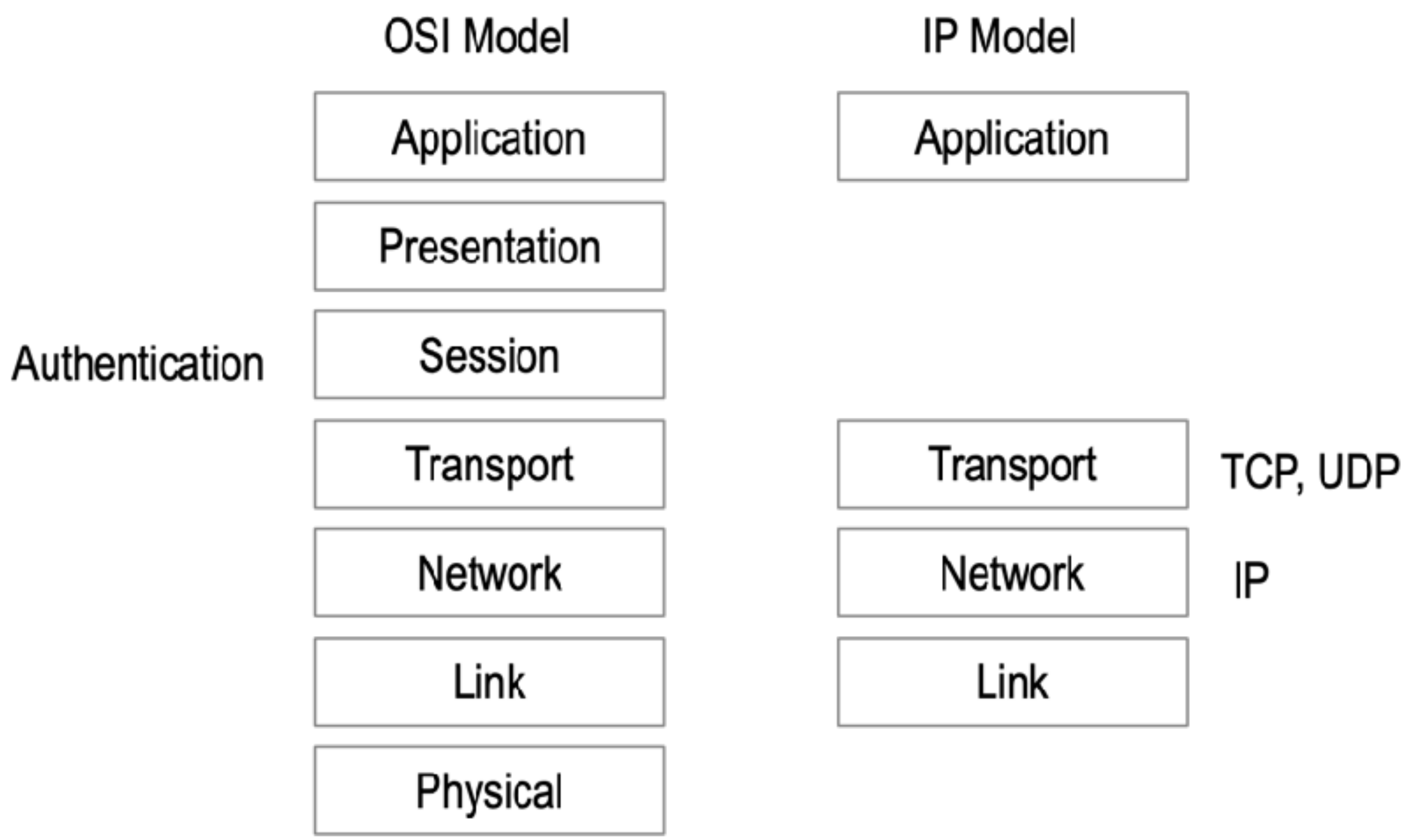
Waist = IP Spanning Layer





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

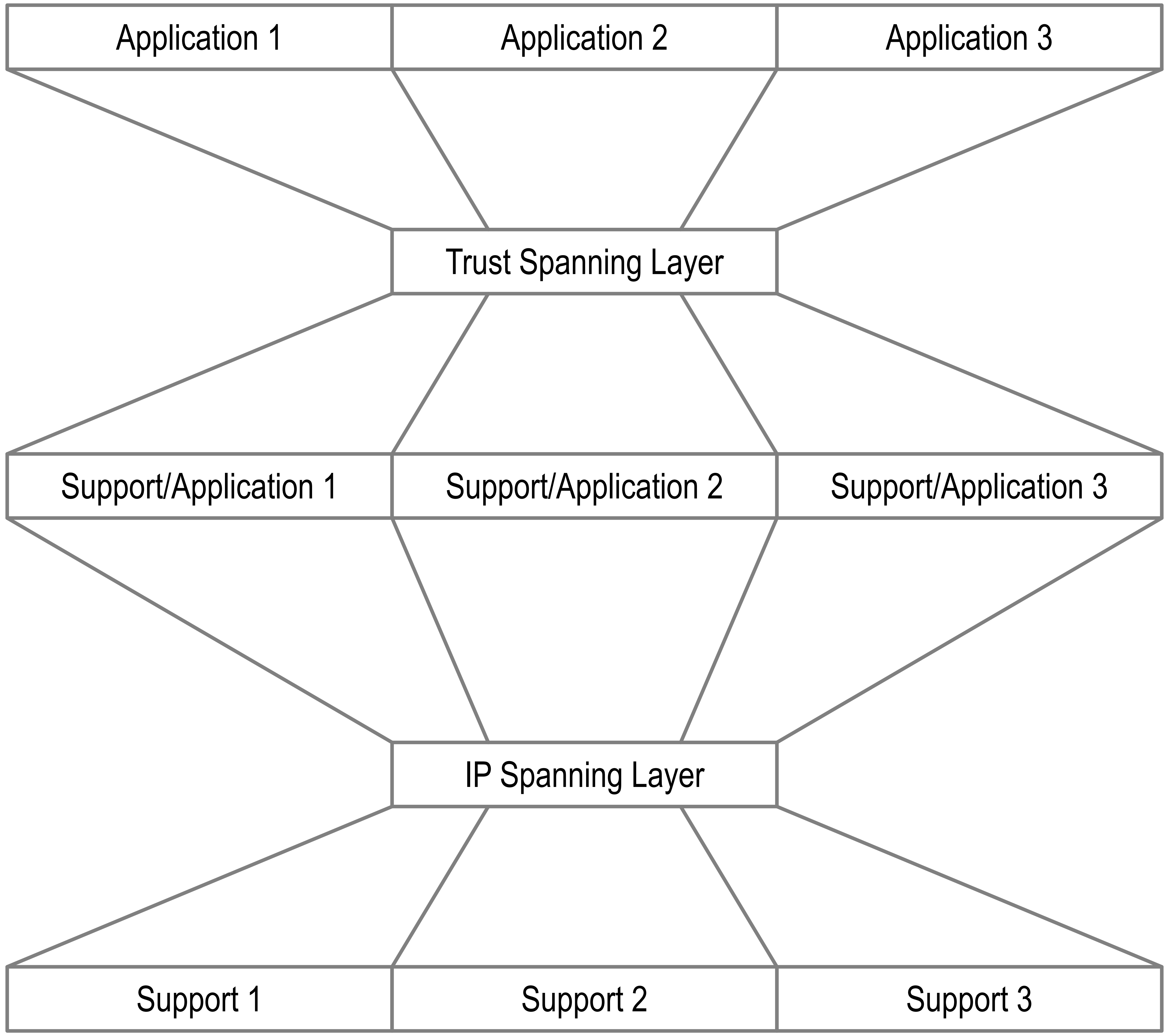
The Internet Protocol (IP) has no *security (trust)* layer.

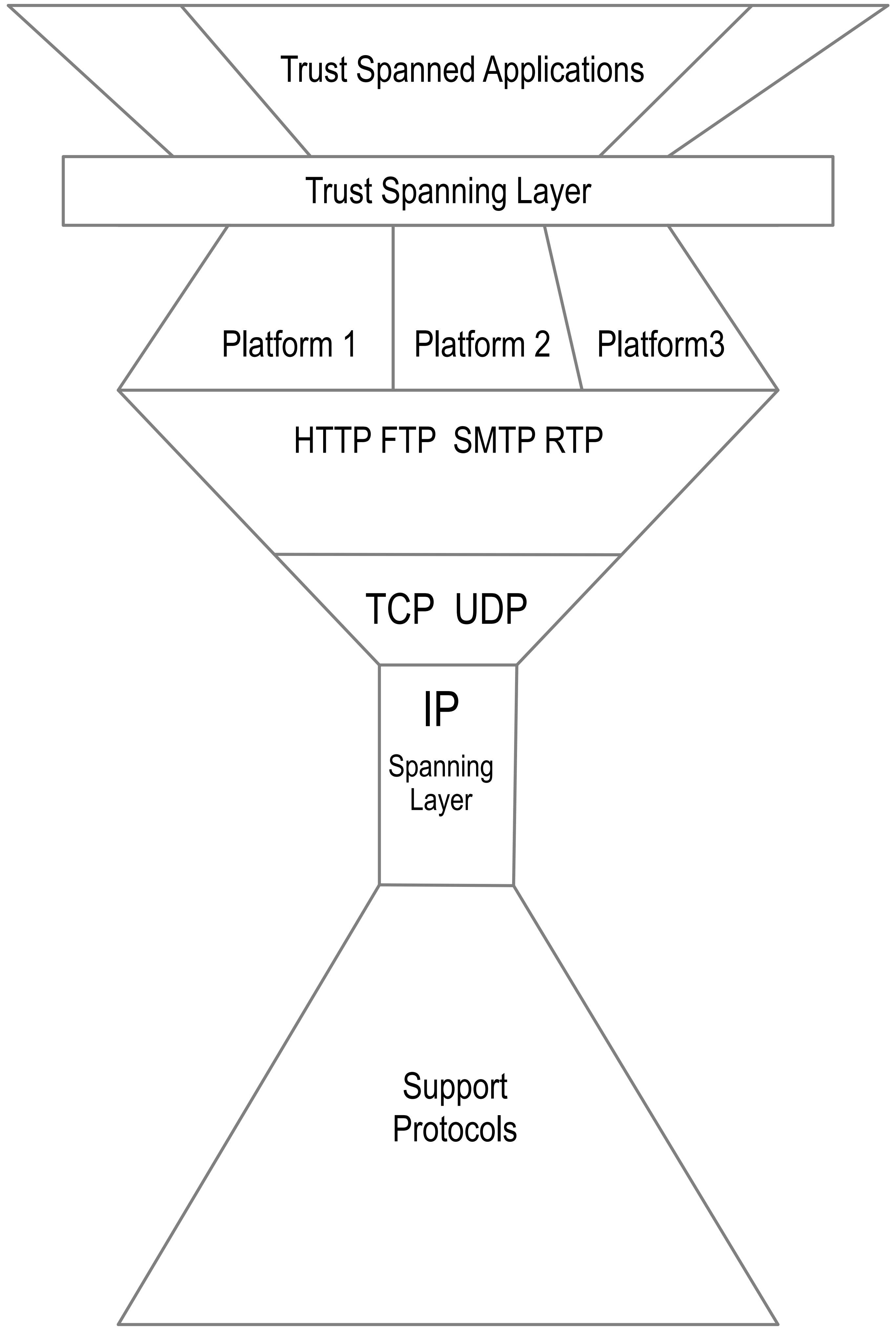


Instead …

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

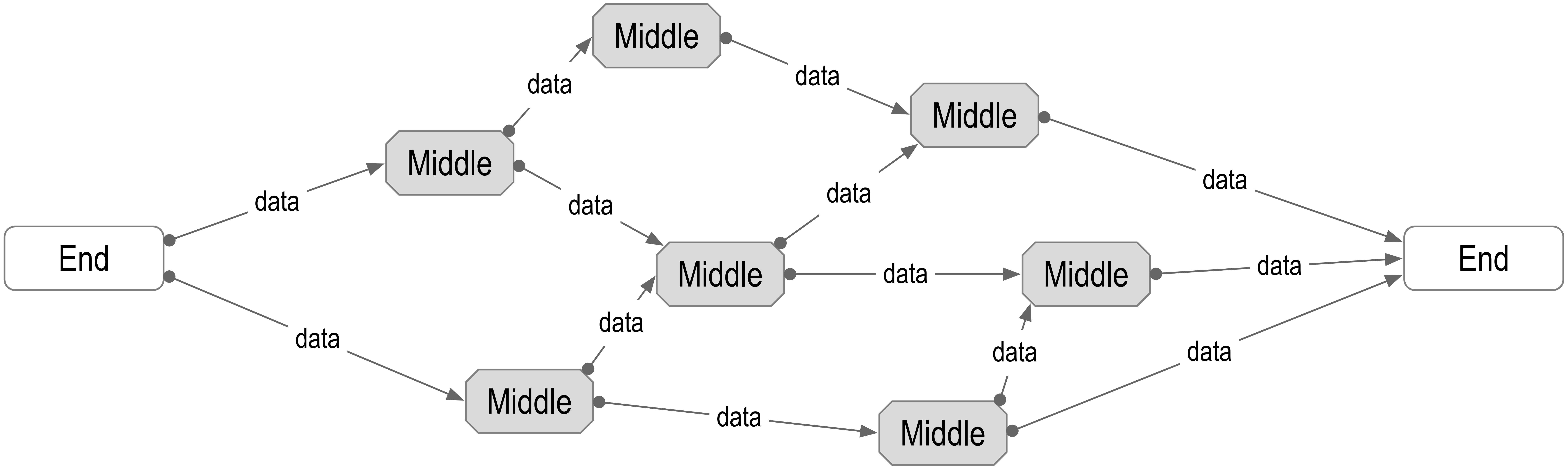
Waist and Neck — Trust Spanning Layer





Dual: End Verifiability and End-Only Viewability

End-to-End Verifiability   Authenticity
Only-at-End Viewability   Confidentiality



Its much easier to protect one's private keys than to protect all internet infrastructure

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

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

End only Viewability: one-data, one-where, one-time by one-body

The myth of unlinkability and the revolution of KERI

"If these out-of-date beliefs are to be called myths, then myths can be produced by the same sorts of methods and held for the same sorts of reasons that now lead to scientific knowledge. If, on the other hand, they are to be called science, then science has included bodies of belief quite incompatible with the ones we hold today." *Thomas S. Kuhn, The Structure of Scientific Revolutions*

security first instead of privacy first

paradigm-shift

privacy and identity theft.

Treating PII as sensitive in order to protect from identity theft confuses a treatment that relieves a symptom of a disease with a cure for the actual disease.

Identity theft (impersonation fraud) results from weak authentication.

It’s only when shared secrets in the form of PII are used as primary authentication factors that privacy has anything to do with identity theft.

Using asymmetric digital signatures as the primary authentication factor can eliminate identity theft, regardless of whether PII protection is in place or not.

right to non-assimilation, not right to privacy
anti-assimilation not de-identification

True *privacy* is largely nonsensical in the context of *shared data*.

If it's shared, it's already NOT private but may be confidential.

We can really only protect the confidentiality of shared data via legal means.

We want technology that allows us to better enforce confidential expectations.

Ultimately, the concern is that others don't exploit us via our data.

Exploitation requires data assimilation.

Anti-assimilation better protects us from exploitation than de-identification.

Examples of Anti-patterns for Bare Selective Disclosure

Any presentation where the discloser is in a location controlled by the verifier.

- Mobile phone tracking data. Live POI tracking.
- Security cameras with facial recognition (or any camera) (https://news.panasonic.com/global/stories/813)
- Credit Card Payment
- Facial biometric with facial recognition
- Parking lot automated license plate recognition
  (https://www.autoweek.com/news/technology/a42444153/california-digital-license-plates-hacked/)
- GeoSpy.AI, Gideon Surveillance AI… etc

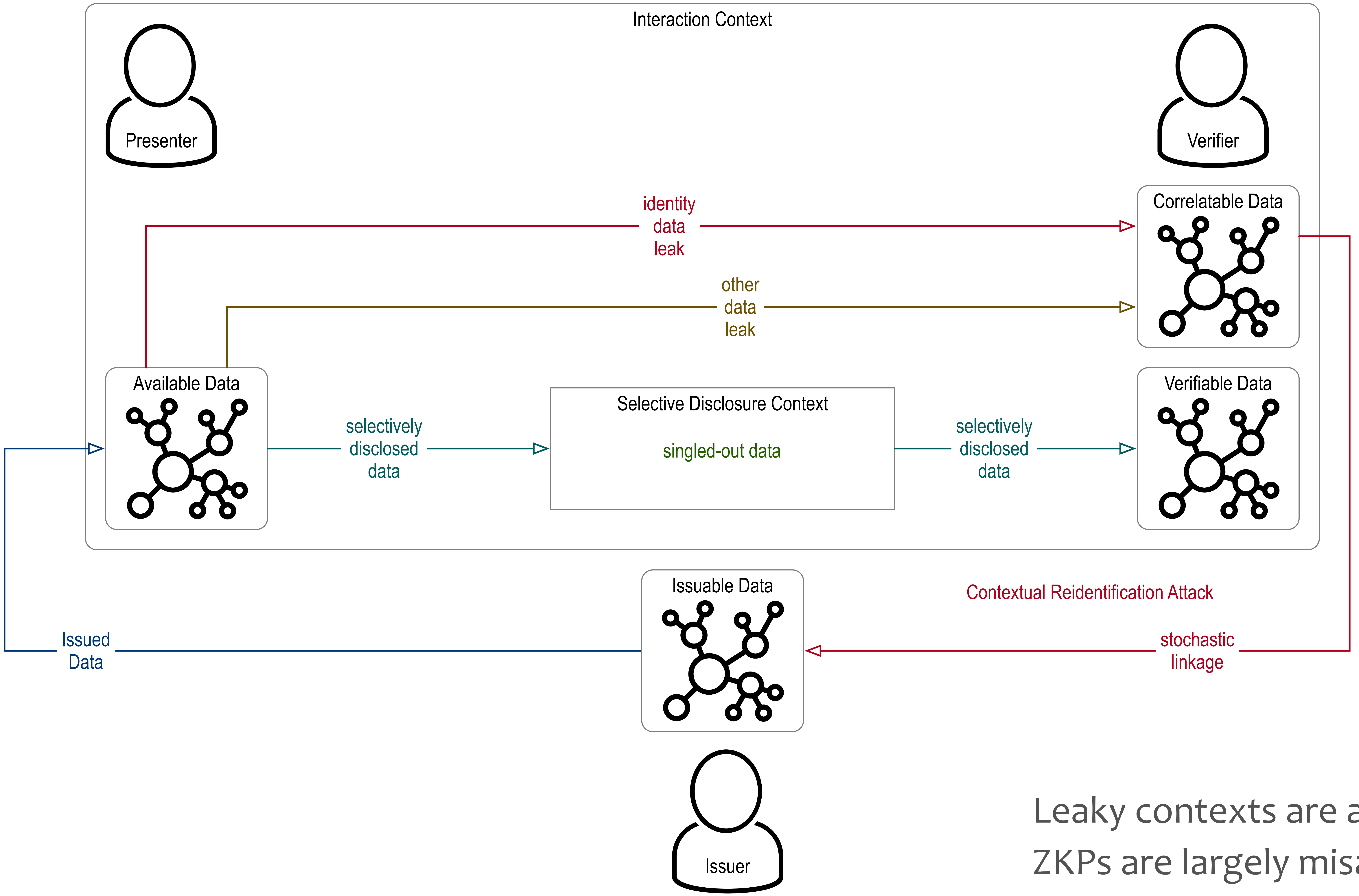
Any presentation on a website that is controlled by the verifier

- IP source address and routing data, web browser fingerprint, and waterfall
- Any purchases on the website

Any presentation on a social application with a social graph of interactions

- Contact tracing apps (https://www.nature.com/articles/s41467-021-27714-6)

Leaky contexts for ZKPs



Leaky contexts are anti-patterns for ZKPs.

ZKPs are largely misapplied in identity applications

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 …

Sustainable Privacy

Sustainable privacy refers to the maintenance and preservation of personal data privacy *over time*.

There are two sides to sustainable privacy:

- How a person maintains their personal data privacy over time.
- How a holder of personal data respects and supports personal data privacy over time.

The difficulty of sustainable privacy is that any information gathering, usage, and sharing system is *leaky*.

Information leaks out over time, thereby gradually eroding the privacy of any data being managed.

The sharing of data is intentional leakage and is, therefore, problematic when viewed from the perspective of sustainable privacy.

Privacy

There are also two fundamentally different but complementary definitions of *privacy* relevant to this discussion.

- The first definition is about the recipient respecting the data privacy concerns of the sender w.r.t. the content disclosed to the recipient. The protection comes from the recipient protecting the data privacy rights of the sender once the recipient has received that data. This first type of privacy protection may be achieved independently of the privacy of the communications channel itself that conveys the content to the receiver.
- The second definition is about the correlatability of the publicly viewable metadata included in the communication. This is called non-content meta-data by the surveillance community. This definition distinguishes between confidential data (meta-data or otherwise) that is not viewable by any third party, not a party to the conversation. Typically confidentiality protection comes from encryption (i.e., cipher text vs. plain text). But an out-of-band (OOB) exchange of information is confidential (not viewable) by a third-party surveillor of the in-band (IB) channel, thus making the OOB exchange itself confidential without encryption.
- Cryptographic solutions alone cannot sustainably protect privacy, w.r.t. either individual data rights or surveillance.
- A comprehensive approach that combines cryptography and legal liability is required.
- Ultimately, accountability on the receiver is necessary to protect the privacy of the discloser in a sustainable fashion.

Practical Elaborations

Authentic and Authenticity

The origin and content of any statement by a party to a conversation are provable to any other party.

Authenticity is primarily about control over the key state needed to prove who said what in the conversation via digital signatures. In other words, it is about secure attribution.

Confidential and Confidentiality

All statements in a conversation are only known by the parties to that conversation.

Confidentiality is primarily about control over the disclosure of *what* (content data) was said in the conversation and to whom it was said (partitioning). Confidentiality is about control over the key state needed to hide content via encryption vis-a-vis the intended parties.

Private and Privacy

The parties to a conversation are only known by the parties to that conversation.

Privacy is primarily about control over the disclosure of *who* participated in the conversation (non-content meta-data = identifiers). More specifically, privacy is about managing exploitably correlatable identifiers, not merely identifiers of *who* but also any other type of identifier in non-content metadata, including conversation (*interaction*) identifiers.

Digital information exchange forces hard gradations on "privacy"

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, secret)

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)

Erosion of 1st Party Data Privacy Rights

- Exploitive use of 1st party data by 2nd parties.
- Sharing of 1st party data by 2nd parties with 3rd parties either overtly or inadvertently.

PbDD: K-Anonymity De-identification

- Current accept *"best"* practice for de-identification is *K-anonymity*.

A release of data is said to have the k-anonymity property if the information for each person contained in the release cannot be distinguished from at least k−1 individuals whose information also appears in the release. *https://en.wikipedia.org/wiki/K-anonymity*

The guarantees provided by K-anonymity are aspirational, not mathematical.

- K-anonymity is broken.
- *Privacy washing* personal data (safe harbor):

  If your personal data as been de-identified using K-anonymity is it no longer considered personal data and my be freely shared. (read the terms-of-use).

K-Anonymity De-identification Continued

Name	Age	Gender	Height	Weight	State of domicile	Religion	Disease
Ramsha	30	Female	165 cm	72 kg	Tamil Nadu	Hindu	Cancer
Yadu	24	Female	162 cm	70 kg	Kerala	Hindu	Viral infection
Salima	28	Female	170 cm	68 kg	Tamil Nadu	Muslim	Tuberculosis
Sunny	27	Male	170 cm	75 kg	Karnataka	Parsi	No illness
Joan	24	Female	165 cm	71 kg	Kerala	Christian	Heart-related
Bahuksana	23	Male	160 cm	69 kg	Karnataka	Buddhist	Tuberculosis
Rambha	19	Male	167 cm	85 kg	Kerala	Hindu	Cancer
Kishor	29	Male	180 cm	81 kg	Karnataka	Hindu	Heart-related
Johnson	17	Male	175 cm	79 kg	Kerala	Christian	Heart-related
John	19	Male	169 cm	82 kg	Kerala	Christian	Viral infection

Name	Age	Gender	Height	Weight	State of domicile	Religion	Disease
*	$20 < Age \leq 30$	Female	165 cm	72 kg	Tamil Nadu	*	Cancer
*	$20 < Age \leq 30$	Female	162 cm	70 kg	Kerala	*	Viral infection
*	$20 < Age \leq 30$	Female	170 cm	68 kg	Tamil Nadu	*	Tuberculosis
*	$20 < Age \leq 30$	Male	170 cm	75 kg	Karnataka	*	No illness
*	$20 < Age \leq 30$	Female	165 cm	71 kg	Kerala	*	Heart-related
*	$20 < Age \leq 30$	Male	160 cm	69 kg	Karnataka	*	Tuberculosis
*	$Age \leq 20$	Male	167 cm	85 kg	Kerala	*	Cancer
*	$20 < Age \leq 30$	Male	180 cm	81 kg	Karnataka	*	Heart-related
*	$Age \leq 20$	Male	175 cm	79 kg	Kerala	*	Heart-related
*	$Age \leq 20$	Male	169 cm	82 kg	Kerala	*	Viral infection

- K-anonymity is broken.

Privacy Washing

- *De-identification provides a personal data* safe harbor.

  If your personal data as been de-identified using K-anonymity is it no longer considered personal data and may be freely shared. (read the terms-of-use).

- Splitting data set into multiple K-anonymous data sets prior to release may be used to privacy wash the data, yet trivially merging the split re-identifies the data.

De-identification Terminology

Attributes in each record of a data set may be classified as

Identifiers (personally identifying information PII attributes)

Quasi-identifiers (vector of attributes where each alone is not identifying but together may be identifying)

Non-identifiers (attributes alone or in combination that are not identifying)

Auxiliary attributes (information not in the data set release)

K-Anonymity is Broken: Re-identification Attacks

K-Anonymity is an NP-Hard problem due to the combinatorics data sets and/or potential auxiliary attributes.

QI Linkage Attack:

Interaction Profiling Attack:

Contextual Linkability Attack:

Quasi-Identifier Linkage Reidentification Attack

Merge Attack

Re-inject identifiers by combining de-identified data sets

Create identifying quasi-identifiers by combining data sets

Create identifying quasi-identifiers by combining auxiliary attributes (https://hdl.handle.net/1721.1/130329) (https://www.nature.com/articles/srep01376)

Generative AI (https://www.nature.com/articles/s41467-019-10933-3/)

Down-coding Attack: (https://www.usenix.org/conference/usenixsecurity22/presentation/cohen)

Hierarchical K-anonymity up-coding to create herds may be systematically down-coded to recreate identifying data even when all attributes are quasi-attributes. Undoes hierarchical generalization. (street, zip, city, state, country) -> (state, country) -> (zip, city, state, country)

Complex Predicate Singling Out (PSO) Attack (GDPR): (https://www.usenix.org/conference/usenixsecurity22/presentation/cohen)

Interaction Profiling Reidentification Attack

Deep learning:

Pseudonym of the two individuals, a timestamp, the type of interaction (i.e., call or text), its direction (i.e., which party initiated it), and the duration for calls in 2-hop interaction network re-identifies over 50% of the individuals.

(https://www.nature.com/articles/s41467-021-27714-6)

Contextual Linkability Reidentification Attack

Uses the statistical correlation of auxiliary attributes obtained from the disclosure context to re-identify the discloser.

A verifier may apply the re-identification correlation techniques described above with auxiliary data obtained at the time of presentation of any selectively disclosed attributes.

Thereby the selective disclosure, whether via Zero-Knowledge-Proof (ZKP) or not, of any 1st party data disclosed to a 2nd party may be potentially trivially exploitably correlatable.

A set of non-selectively disclosed attributes (auxiliary data) obtained from the context of the disclosure may be sufficient to re-identify the discloser despite selective disclosure.

A contextual linkability attack may thereby trivially defeat the cryptographic unlinkability provided by selective disclosure mechanisms, including those that use ZKPs.

Contextual Linkability Reidentification Continued

The vulnerability stems from the fact that the verifier may structure the context of the presentation to provide sufficient auxiliary data that the combination of contextual auxiliary data and selectively disclosed data is identifying.

Verifier control over the context of a selective disclosure presentation and the associated capture of auxiliary attributes may create quasi-identifiers or even identifiers that may be combined with selectively disclosed attributes in such a way as to re-identify the associated subject of the selectively disclosed attributes.

Thus, selective disclosure mechanisms (including ZKPs), by themselves, are inadequate for privacy protection.

Any unconstrained use of a selectively disclosed set of attributes may be re-identifiable unless the discloser takes care to both protect from contextual linkability and impose a contractual liability on any use of that data.

Bare selective disclosure implicitly grants the disclosee (verifier) a safe harbor to use, assimilate, and re-identify the disclosed data.

Examples of Anti-patterns for Bare Selective Disclosure

Any presentation where the discloser is in a location controlled by the verifier.

- Mobile phone tracking data. Live POI tracking.
- Security cameras with facial recognition (or any camera) (https://news.panasonic.com/global/stories/813)
- Credit Card Payment
- Facial biometric with facial recognition
- Parking lot automated license plate recognition
  (https://www.autoweek.com/news/technology/a42444153/california-digital-license-plates-hacked/)
- GeoSpy.AI, Gideon Surveillance AI… etc

Any presentation on a website that is controlled by the verifier

- IP source address and routing data, web browser fingerprint, and waterfall
- Any purchases on the website

Any presentation on a social application with a social graph of interactions

- Contact tracing apps (https://www.nature.com/articles/s41467-021-27714-6)

Interaction Contexts that defeat ZKP cryptographic unlinkability

Any interaction where the person is physically present at the time of presentation
Any interaction that uses conventional payment rails
Any interaction that uses a conventional mobile phone
Any interaction over a publicly routable network
Any virtual private network that routes through a treaty country

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

Bare Selective Disclosure

Because most presentation contexts are under the control of the 2nd party (verifier), the verifier needs merely to structure that context with enough quasi-identifier attributes (auxiliary data) to re-identify the presenter, which in turn would enable the 2nd party to link the de-identified presenter back to the issuer with the presentation details thereby defeating cryptographic unlinkability.

Cryptographic unlinkability is the unique reason to use a ZKP in the presentation in the first place.

This does not mean that there are no corner conditions where the presentation context is sufficiently under the control of the presenter (1st) party such that the presenter can structure the context to prevent the verifier from correlating any other quasi-identifiers, but none of the standard use cases for cryptographic unlinkability satisfy that condition.

Bare selective disclosure as a privacy mechanism is relegated to the narrow corner conditions where there is zero contextual linkability by the 2nd party disclosee (verifier) at the time of presentation.

Selective Disclosure as Naive K-anonymity

Correctly understood, selective disclosure is a naive form of K-anonymity performed by the discloser (presenter).

The discloser is attempting to de-identify their own data.

Unfortunately, such naive de-identified disclosure is not performed with any statistical insight into the ability of the verifier (receiver) to re-identify the selectively disclosed attributes given the contextual attributes that are also disclosed (inadvertently) at the time of presentation and under the control of the verifier.

Because most if not all standard use cases for selective disclosure assume a presentation context that is under the control of the verifier, a malicious verifier can restructure that context to statistically guarantee correlation and defeat the selective disclosure with or without a ZKP.

As a result, many of the standard use cases for selective disclosure (with or without ZKPs) in verifiable credential (VC) presentations are examples of anti-patterns for the use of selective disclosure.

The discloser may have a false sense of protection from selective disclosure that results in much more promiscuous disclosure.

Summary of Contextual Linkability Vulnerability

The core defect of any K-anonymity-like approach, including selective disclosure, is that there is no apriori way for the discloser to establish if any selectively disclosed attribute is an identifier, quasi-identifier, or non-identifier because all attributes are potentially identifying given auxiliary data, especially, that obtained from the context of the disclosure.

Any non-aggregated 1st party data shared with a 2nd party may be easily re-identifiable because there is no herd privacy. The data is directly attributable to the one and only one 1st party.

The act of sharing forms a sharing disclosure context that may be structured by the 2nd party to provide easily correlatable contextual auxiliary data that enables re-identification via a contextual linkage attack.

Therefore, naive K-anonymity-based mechanisms such as selective disclosure, including ZKPs, that provide so-called cryptographic unlinkability may be trivially linkable by statistical re-identification methods using contextual auxiliary data.

As a result, bare (naive) selective disclosure alone provides no guarantee of privacy protection to the discloser.

Trade Space

Selective disclosure mechanisms are not free, especially ZKPs.

This induces a trade-space between friction of adoption and privacy protection.

Any verifier sophisticated enough to verify a ZKP is sophisticated enough to defeat it using contextual linkability.

Comprehensive Protection Mechanism

The only practically viable protection against the 2nd-party correlation of non-aggregated 1st-party data is pre-disclosure contractual protection by imposing liability on the 2nd party disclosee and strict post-disclosure chain-link confidentiality on any downstream disclosees or other users of that data, including any later assimilation or aggregation.

Chain-link confidentiality requires that 2nd parties not aggregate 1st party data, de-identified or not (selectively disclosed or not), without the consent of the 1st party.

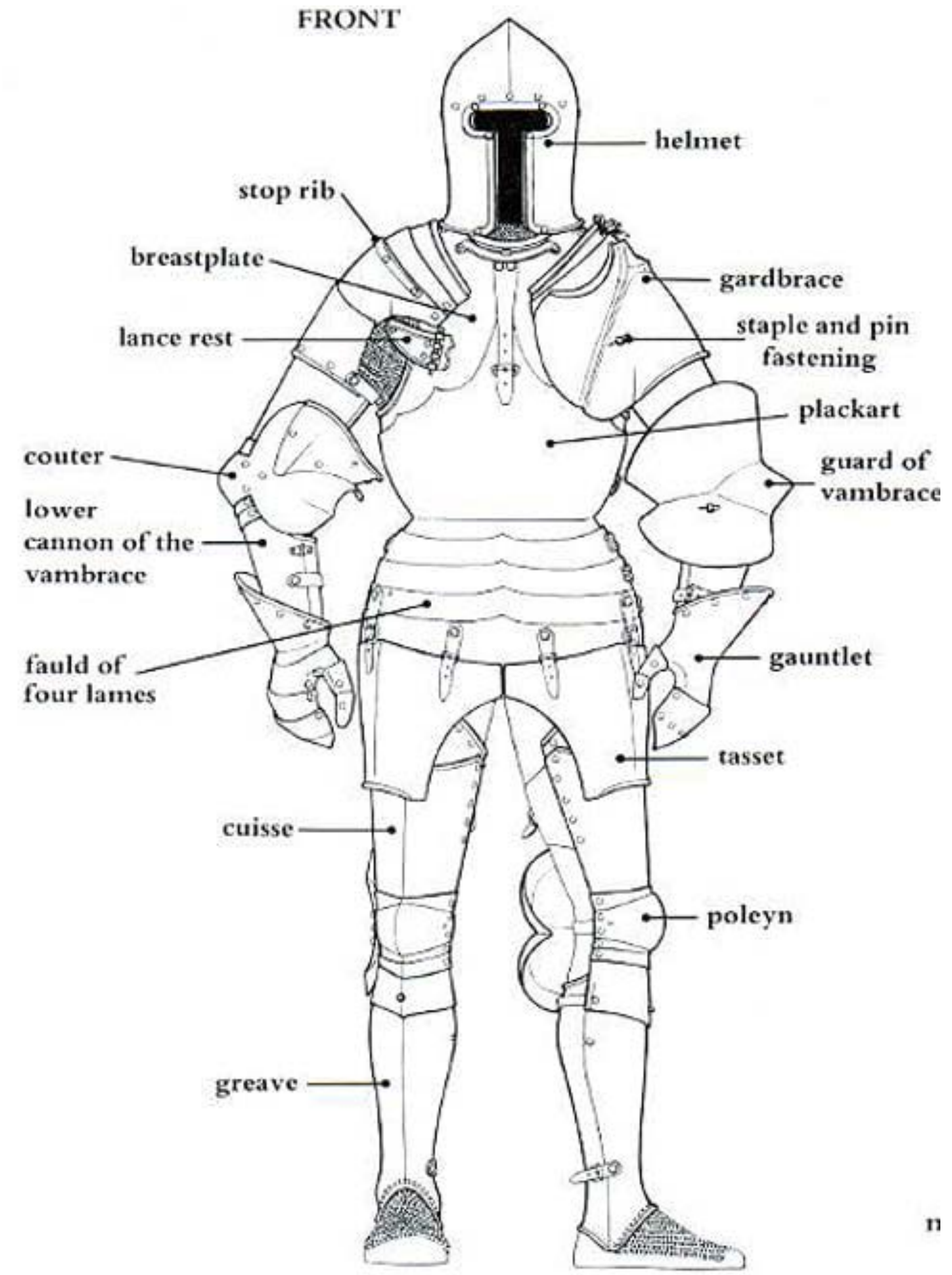
The only sustainable privacy protection mechanism of 1st party data disclosed to a 2nd party, even when selectively disclosed (via ZKP or not), is contractually protected disclosure via chain-link confidentiality.

Any selective disclosure is ineffective unless performed within the confines of a contractually protected disclosure that incentivizes the disclosee (verifier) to protect that disclosure (counter-incentive against the exploitation of that discloser).

Questions

Armor

Preventing *wounds* especially *fatal* *wounds*



Remove even one component protecting a vital area
and the adversary will target the unprotected area to the exclusion of all else.

Whitepapers

Sustainable Privacy

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

Secure Privacy, Authenticity, and Confidentiality

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

https://github.com/SmithSamuelM/Papers/blob/master/presentations/SPAC_Overview.web.pdf

Clandestine vs Covert Mechanisms

The nesting of contexts extends the covert analogy.

Given *A* has a generic end-wise routing relationship context with *B*, that *A* uses for a multitude of confidential interactions with *B* where each interaction uses a dedicated interaction relationship context between *A* and *B.*, then the end-wise routing context provides cover for the end-wise interaction contexts.

The traffic over the general routing context is another form of herd privacy. This enables *A* *and *B* to conduct sustainable hide-in-plain-sight operations that minimize the exploitable correlatable information.

Each of the relatively public long-term generic communication contexts (covert) and long-term generic routing contexts (covert) provide nested covers to the really valuable private short-term interaction contexts (clandestine).

Clandestine vs Covert Mechanisms

In comparison, a more covert operation approach may be more robust to leakage and hence more sustainable. For example, there are various ways to provide the equivalent of a "cover" identity for communications traffic.

Specifically, with regard to the protocols above, parties *A* and *B* have several relationship contexts. They each have a hop-wise communications context with an intermediary, e.g. *A* with *C* and *B* with *D*.

To the extent that *C* and *D* have many users that have well-known legitimate "public" uses of *C* and *D*, then *C* and *D* each have a cover identity with respect to their respective relationships with *A* and *B*. For example, if the only time anyone uses *C* is to conduct some private activity, then the use of *C* by itself is suspect and provides correlatable information.

Specifically, suppose that *C* is a VPN, and the only time *A* uses *C* is to communicate with a crypto-currency exchange in Cyprus in order to avoid the FATF KYC rules for exchanges in FATF-compliant countries then, anytime *A* uses *C* the use is exploitable information. Whereas if *A* uses *C* for all communications, then the occasional communication to Cyprus is concealed by the cover of the other activity.

Likewise, if all users of *C* use *C* for all their traffic, then they provide herd privacy to every other user. But if most of the users of *C* only use *C* to conceal transactions for which they want more privacy (i.e., clandestine), they make the mere use of *C* itself a correlatable signal that exposes their clandestine operation.

Re-Identification

To elaborate on the futility of purely clandestine methods for sustainable privacy, consider the problem of de-identification and re-identification of data.

It was long thought that de-identification or anonymization of data could provide privacy using a technique called (k-anonymity)[https://en.wikipedia.org/wiki/K-anonymity].

Recent research has shown that fully de-identified sparse datasets can be merged to re-identify the data (re-identification)[https://www.nature.com/articles/s41467-019-10933-3/] (Lie of Anonymous Data)[https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/].

In 2022, this was further extended to what is called a down-coding attack which enables the re-identification of data even when every field is a quasi-identifier, i.e., there is no personally identifying information in the dataset, (down-coding attack)[https://www.usenix.org/system/files/sec22-cohen.pdf]. Indeed the ease and pervasiveness by which de-identified data may be re-identified have resulted in the US FTC (Federal Trade Commission) issuing a warning that those who share de-identified databases and purport that merely through de-identification that the privacy rights of the associated persons are protected may be in violation of the laws regulating the use and sharing of sensitive data. (FTC Illegal Use and Sharing)[https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal]

AIDs as Unbounded Term Identifiers

Long-term public keys and short-term public keys.

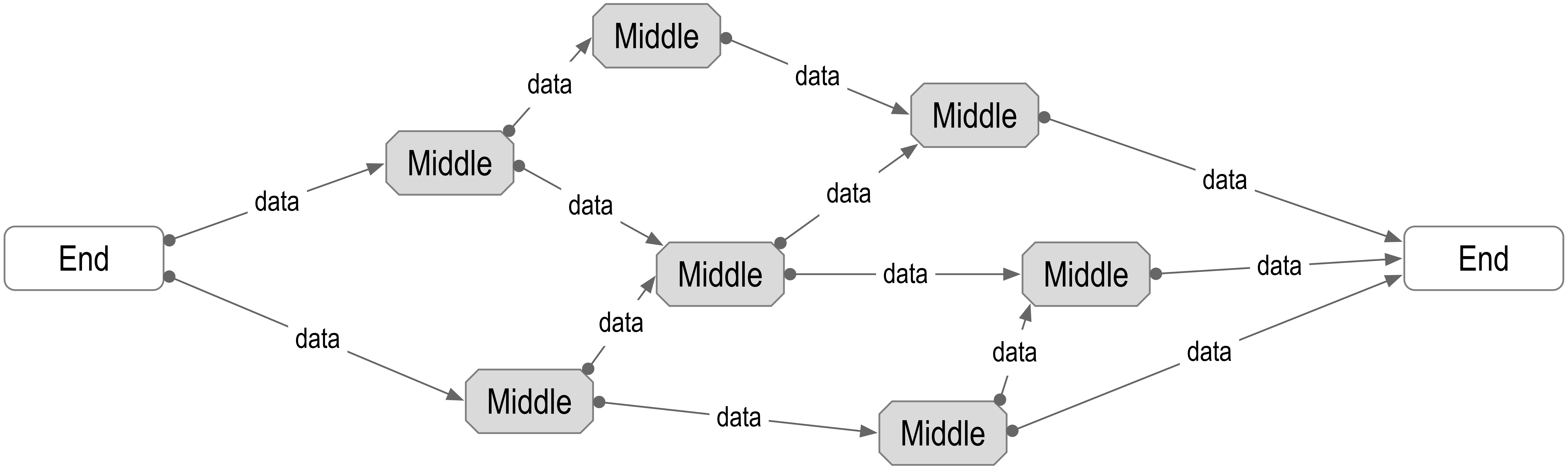
Many public key cryptographic algorithms employ the concept of ***long-term*** public keys and ***short-term*** public keys. Often long-term keys have less exposure than short-term keys so they can maintain their cryptographic strength longer.

Typically this is to better manage the friction of key exchange where higher friction authentication of long-term keys is used to enable or bootstrap cryptographic operations using short-term or ephemeral keys.

One simplification that results from this approach is that many protocols can be simplified to remove repeated setups using ephemeral (short-term) keys whose purpose is to reduce the exposure of the long-term keys.

Dual End Verifiability and End-Only Viewability

End-to-End Verifiability *of Authenticity*
Only-at-End Viewability via Confidentiality



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

End only Viewability: one-data, one-where, one-time by one-body

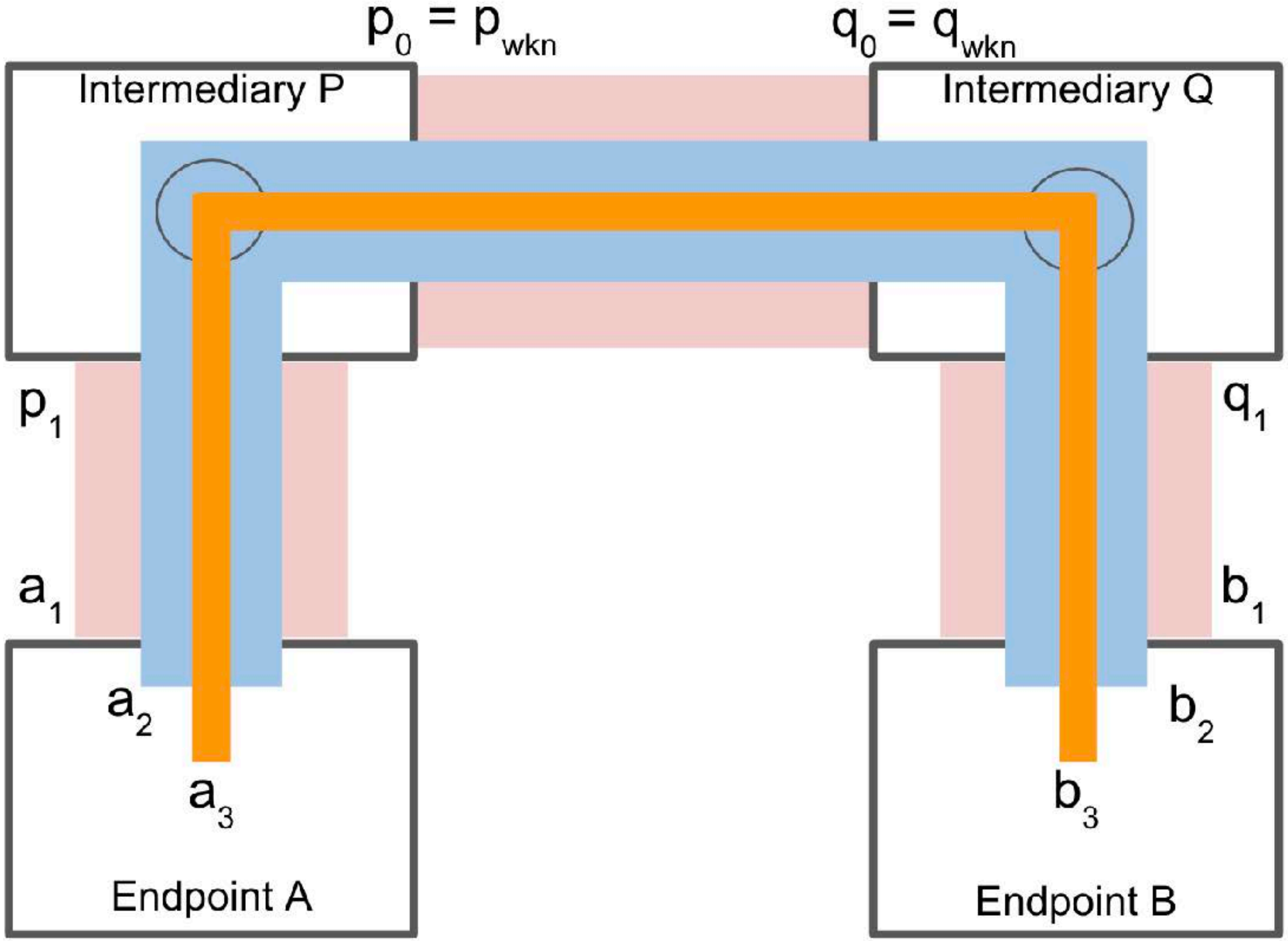
If the edges are secure, the security of the middle doesn't matter.

Zero-Trust-Computing

Its much easier to protect one's private keys than to protect all internet infrastructure

TSP (SPAC) Protocol

Triple-nested tunneling protocol that minimizes surveillable metadata



covert vs. clandestine surviellability

Identity Theft Threats

Multi-step recursive privilege elevation attack (authentication and authorization).

The attacker compromises weak access credentials on low-value targets that allow it to elevate its privileges in order to compromise a higher-value target until it finally has the access credentials of a treasure trove.

An example of this would be to compromise the VPN login of some customer or employee of some company that allows an attacker to compromise some other employee's VPN login to a connected company and so on until it captures access credentials to a connected company's treasure trove.

It starts with what is called an edge attack on the weakest company.

The elevation mechanism often leverages what is called a BOLA or BUA.

These are not privacy weaknesses but authentication-based authorization weaknesses.

"Hackers can use data stolen from companies with weak security to target employees and systems at other companies, including those with strong security protocols. ... the data ecosystem has become so vast and interconnected that people are only as safe as the least secure company that interacts with any company that has access to their data. That "least secure company" does not even need to have access to the consumer's data. … There were 5,212 confirmed breaches in 2021, which exposed 1.1 billion personal records across the globe"

To summarize, a given trust domain is only as strong as the weakest connected trust domain (in which connected is recursively applied).

https://www.apple.com/newsroom/pdfs/The-Rising-Threat-to-Consumer-Data-in-the-Cloud.pdf)

https://heimdalsecurity.com/blog/what-is-broken-object-level-authorization-bola/

https://github.com/OWASP/API-Security/blob/master/2019/en/src/0xa2-broken-user-authentication.md) https://www.traceable.ai/blog-post/a-deep-dive-on-the-most-critical-api-vulnerability-bola-broken-object-level-authorization

https://owasp.org/ww-project-api-security/)

Exploiters

State Actors (3rd party):

The primary incentives for state actors are political, but some like North Korea are also monetary.

State actors may use any combination of attacks to surveil, regulate, and persecute all first parties, second parties, and intermediaries with virtually unlimited resources and the ability to cause harm.

Because of the virtually unlimited resources and techniques that state actors can apply we will treat them as out of scope for mitigation for the time being. That does not mean we will not consider state-actor resistant mitigations but to attempt state-actor proof mitigations would likely take us down rabbit holes that we can never return from.

Identity Thieves (3rd party):

The primary incentive for identity thieves is monetization through asset theft. Typically either directly through the capture of access credentials to assets or indirectly through the sale of personally identifying information (PII) that may be used to capture access credentials. Another primary monetization strategy is ransomware of either access credentials or PII that may be used to capture access credentials or simply sensitive PII such as health data.

Aggregators (3rd party, 2nd party, 1st party):

The primary incentive for aggregators is to sell data to advertisers. This means profiling groups of potential customers in attractive demographics. This profiling may be entirely statistical. There are several classes of aggregators. These include:

Intermediaries (3rd party):

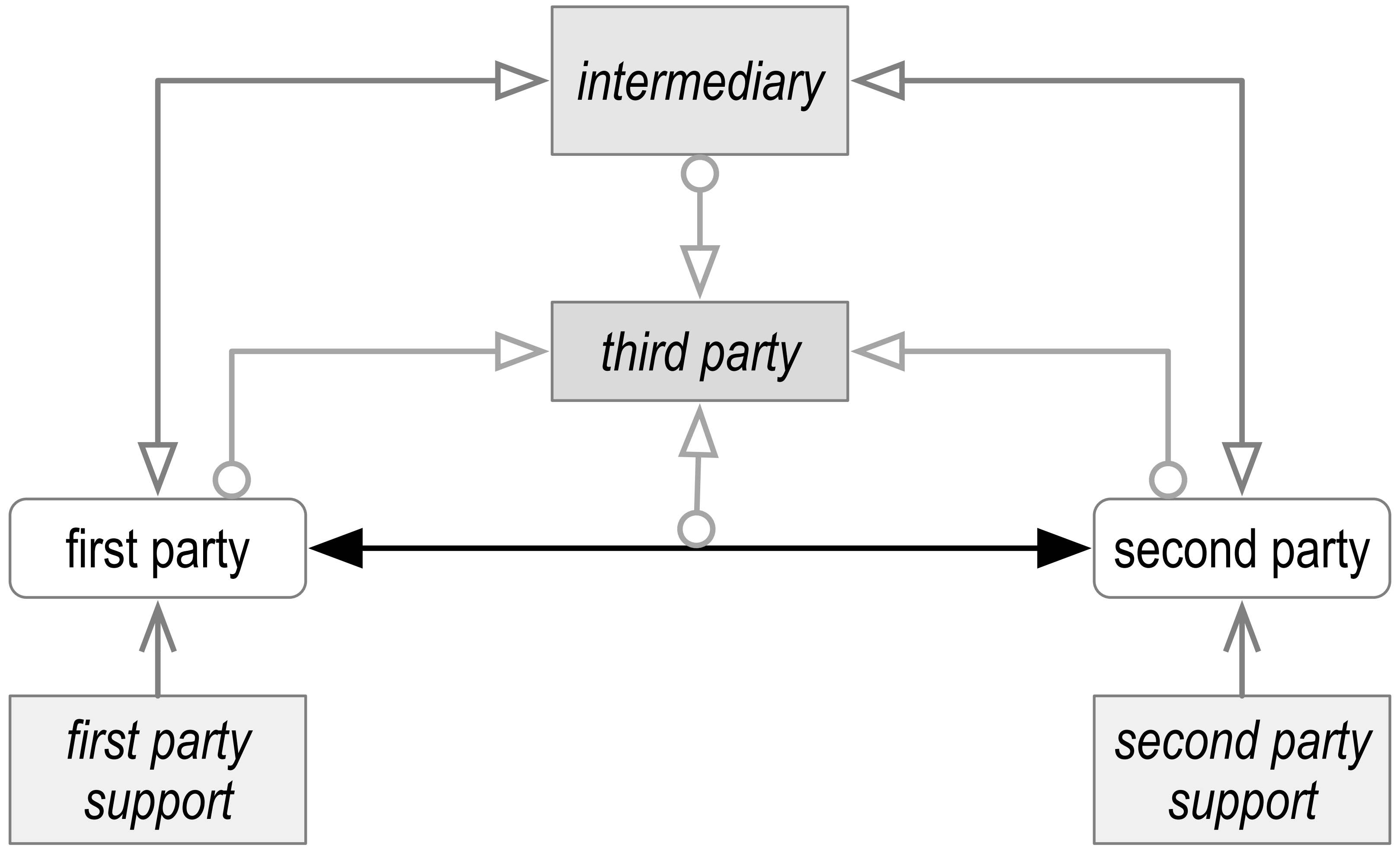
* Search as an aggregator
* Cloud provider as an aggregator
* ISP as an aggregator

Platforms (2nd party)

* Colluding 2nd parties as aggregators

Inadvertent (1st party)

* Inadvertent colluding 1st party as an aggregator via web cookies



Identity Theft Mitigations

* Use strong authentication by 2nd parties of any first party at any step along a multi-step recursive privilege elevation attack. In any multistep recursive privilege elevation attack any step that has strong authentication with individually signed requests for authorization will stop the attack from proceeding.

* Use strong authentication by any 2nd party of any 1st party for any exploitable use of first-party credentials, whether those credentials be credit card, bank account, or access to sensitive data.

* Use strong authentication (zero-trust data in motion and at rest) at any party holding a treasure trove. Strong authentication is also state-actor resistant.

* Get rid of treasure troves of access credentials by using decentralized trust domains (DPKI). This means passwordless security with strong key rotation mechanisms. This is also state actor resistant.

Third-Party Aggregator Threats and Mitigations 1

Search as an intermediary (3rd party).

In this case, an internet search engine is able to track the click-throughs of a successful search result. This enables the search engine to monetize the 1st party searcher by correlating the meta-data of the incoming client browser with the 2nd party endpoint resulting from the search.

* Mechanisms:

  - 1st party permissioned surveillance of first party metadata collected by 3rd party search intermediary and sold to other 3rd parties

* Mitigations:

  - Use VPN in combination with a partitioned 1st party identifier such as a random email address

  - Use a search engine that contractually protects 1st party search metadata.

Third-Party Aggregator Threats and Mitigations 2

Cloud data storage provider as an intermediary (3rd party).

In this case, all 1st party content data stored in the cloud may be anonymized and re-correlated to provide monetizable advertising campaign pools.

* Mechanisms:

- First-party permissioned surveillance of first-party content data by 3rd party cloud provider intermediary and sold to other 3rd parties.

* Mitigations:

- Use cloud storage providers that use end-to-end encryption (first-party confidential content data)

- Use cloud storage providers that contractually protect 1st party content data.

Third-Party Aggregator Threats and Mitigations 3

Internet Service Provider (ISP) as an intermediary (3rd party).

In this case, ISP has access to all traffic routed through it for 1st party client connections to any 2nd party. ISP can anonymize and then re-correlate into monetizable advertising campaign pools.

* Mechanisms:
    - Non-content Metadata (routing and billing) identifiers. In the USA for example any anonymized data (both metadata & content) is aggregation permissible for any ISP.
    - Mobile device location tracking.
* Mitigations:
    * Use an ISP that contractually protects user metadata
    - Use VPN that contractually protects user metadata. A VPN provides herd privacy relative to ISP tracking of the source to 2nd party destinations.
    - There is no mitigation for mobile device tracking by mobile service providers except to turn off the mobile device.
    - Use distributed decentralized confidential network overlay to make metadata harder to correlate. This could include onion or mix network routing such as TOR, Elixxir, MainFrame, and DIDComm Routing. In general, a decentralized network overlay is difficult to incentivize and as a result, may have relatively low adoptability when compared to a VPN.
    - Use information-theoretic secure routing. An example would be random walk routing. Of all the mitigations, this one is state actor resistant. Information-theoretic secure routing, however, has similar adoptability problems as a decentralized confidential network overlay.

Second- and First-Party Aggregator Threats and Mitigations

Monetized via advertising. (Assuming content data is confidentially encrypted between first party and second party)

Second Parties as Aggregators:

- Mechanism:
  - First-party content data (also non-content metadata when available), not as a 3rd party surveillor (intermediary)
  - Statistical regression of anonymized content data by a large second party or by multiple colluding 2nd parties
- Mitigation:
  - Don’t use 2nd parties that aggregate without permission (anonymization is no protection)
  - Use contractually protected disclosure and/or selective disclosure

First Party as Inadvertent Aggregator:

- Mechanism:
  - Browser cookies makes 1st party browser an inadvertent permissioned intermediary that can leak both non-content metadata and content data to second parties and/or intermediaries
- Mitigation:
  - Don’t use browsers in a way that supports tracking first-party data via cookies by 2nd parties or intermediaries

Risk Mitigation Prioritization

Risk Rating and Ranking:

Magnitude of harm multiplied by the likelihood of harm versus the relative cost of mitigation as a percentage of available resources to mitigate all harms

Identity theft has very high harm magnitude with moderate likelihood but potentially low cost of mitigation via strong authentication and strong confidentiality

Aggregation harm per exploiter is small with very high likelihood so pick from privacy mitigations that are cost-effective

The internet is broken primarily because of identity theft.

The infrastructure changes needed to fix identity theft will enable easier adoption of the changes needed to better protect against aggregators.

Surveillance Privacy Problem

We can have strong authenticity and confidentiality (of anything but addresses) but weaker privacy w.r.t addresses (identifiers). Beyond a certain point, better privacy over addresses becomes impractical because the world needs addresses for routing and billing on public infrastructure and will always need them.

Privacy, as non-correlatable identifiers (metadata) will always be difficult.

Whereas, privacy as control over one's data rights is easier because it's not about routing or billing.

For the purposes of protocol design the definitions of confidentiality and privacy that are most suitable are the surveillance definitions because these are primary to the trade-space of PAC.

Historical Basis for Surveillance Privacy

Historically, an address of any kind (including the original postal address) exists for two main purposes.

1. So that stuff can get routed (delivered) to that address as a destination via public roads.

2. So that legitimate parties can tax or bill efficiently other parties at any or all addresses.

In the electronic communication world, the same applies. Addresses need to be public so that communications can be routed to destinations over multiple disparately owned, controlled, and regulated communications infrastructures (largely public-regulated monopolies). Likewise, the main mechanism for billing for communication services rendered is address based. So addresses have to be public, not confidential, not only so that stuff can get routed to those addresses but also so they can be the destination for bills to pay for the communication itself. So pragmatically, the legal surveillance world respects that these two purposes (routing and billing) require identifiers (addresses) that must need be public and eaves-droppable.

This is merely a logical, practical extension of property rights w.r.t. unreasonable search. The right to be protected from search only extends to what is not viewable behind closed doors. Anything viewable from a public street is fair game with no protection. Likewise to some extent an automobile or delivery van. What's locked in the trunk or the back of the van (unless it's making noise hearable by a bystander) may be protected. Where it goes on a public street is not protected, and its license plate is a publically viewable address proxy.

As a result, both practically and legally, all routing and billing mechanisms assume to a large degree, that addresses are not private. Anyone trying to build a house and then telling the post office that it can't assign them a public address or expecting that anyone will build infrastructure to support getting stuff delivered but not using public streets will likely fail. Imagine the cost of supplanting public streets with a totally private conveyance system (air space, sea space, and space space are public already).

If one wanted to build a totally private alternative to the public road network, then maybe automobiles and vans on private roads wouldn't need license plates (oh wait these are called toll roads, and they need a billing address) so not.

ToIP Design Goals

Establishing trust between parties requires that each party develop confidence in the following properties of their relationship:

Authenticity

Is the receiver of a communication able to verify that it originated from the sender and has not been tampered with?

Confidentiality

Are the contents of a communication protected so that only authorized parties have access?

Privacy

Will the expectations of each party with respect to the usage of shared information be honored by the other parties?

Note that, in some trust relationships, confidentiality and privacy may be optional. Thus our design goal with the ToIP stack is to achieve these three properties in the order listed.

The ToIP design goals provide an order of importance. The design goals indicate that one should start with high authenticity, then high confidentiality, and then as high as possible privacy, given there is no trade-off with respect to the other two.

https://github.com/trustoverip/TechArch/blob/main/spec.md#61-design-goals

Privacy and Confidentiality Legalese

The terms confidential and private also have distinct legal definitions.

The legal definition of confidentiality, however, is consistent with both the surveillance definition and the design goal definitions above. Confidentiality law is about contractual agreements governing the disclosure of data by one party to another.

The legal definition of privacy, on the other hand, is not so consistent. The regulatory surveillance law definition differs from the privacy rights regulatory law definition.

The former is about drawing the line between non-content metadata and content data in order to be classified as either searchable or not (see https://www.lawfareblog.com/relative-vs-absolute-approaches-contentmetadata-line and https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance/)

The latter is mainly about protecting personal data rights by data holders, controllers, and processors such as GDPR (see https://gdpr-info.eu).

Confidentiality law can be used better to protect personal data rights. For example, the well-known concept called [chain-link confidentiality](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045818), circa 2012, details how one can protect the data privacy concerns of the sender via contractual confidentiality law.

ACDCs, for example, use the well-known [Riccardian Contract](https://iang.org/papers/ricardian_contract.html) formalism, circa 1996, to support chain-link-confidential through what is called contractually protected disclosure.

Survelliance Legalese

Physical Search

A physical address is a public identifier used for routing and taxing.

Viewing who enters the home from outside via public street is unprotected. (subpoena)

Viewing what happens behind closed doors inside the home is protected. (warrant)

Information Search

Relatively weak legal protection (subpoena) for identifiers (non-content meta-data) because identifiers are needed for public routing and billing.

Relatively strong legal protection (warrant) for content because the content is not needed for public routing and billing.

Privacy Protection as Protection from Exploitation

We define privacy protection as protection against the ***exploitation of correlatable identifiers*** (metadata).

The goal becomes limiting the exploitation via exploitably correlatable identifiers (metadata).

If we can protect against ***exploitation*** derived from the correlation of identifiers, we may achieve effective privacy.

Protection against exploitation via correlation provides a more gentle trade space than mere protection against correlation.

The former is practical and amenable to cost-benefit analysis, but the latter is largely impractical.

Strong End-Only-Viewable Confidentiality

Use the 3-party model where:

1st party is the sender,

2nd party is the intended receiver

3rd party is any unintended receiver.

A system with strong end-only viewable confidentiality may have the following properties:

- 3rd party non-viewability
- 1st party non-viewability (this protects 1st party from liability wrt to 2nd party and protects 2nd party from exploit by 1st party) (see appendix for a more detailed description of this property)
- 2nd party partition-ability by 1st party
- Detectable leakage (2nd party to 3rd party)
- Detectable collusion of 2nd party against 1st party (2nd party with 2nd party, or 2nd party with 3rd party)
- Detectable collusion of 1st party against 2nd party (1st party with another 1st party relative to same 2nd party or 1st party with 3rd party)

Best Authenticity (Secure Attribution) SUF-CMA

The standard for strong public key signing algorithms is SUF-CMA (Strong UnForgeability under Chosen Message Attack).

When a digital signature has SUF-CMA with at least 128 bits of cryptographic strength then it is computationally infeasible to forge a signature or to discover the private key by choosing messages.

The Libsodium implementation of the NaCL Ed25519 signature scheme has SUF-CMA (See Provable Security of Ed25519 https://eprint.iacr.org/2020/823.pdf).

In comparison, the popular ECDSA signature scheme only has the weaker EUF-CMA (Existential UnForgeability under Chosen Message Attack). Any scheme with SUF-SMA also has EUF-CMA This relative weakness of ECDSA has already been exploited in bitcoin. Consequently, some additional care must be taken when using signature schemes, like ECDSA, that are not SUF-CMA.

Strong Authenticity Baseline

Security properties of Ed25519 in libsodium:

scheme	EUF-CMA	SUF-CMA	S-UEO	M-S-UEO	MBS
Ed25519-LibS	X	X	X	X	X

S-UEO (Strong Universal Exclusive Ownership) and M-S-UEO (Malicious Strong Universal Exclusive Ownership) properties provide additional resiliency against key substitution attacks. Whereas the MBS (Message Bound Security) property ensures a given signature verifies a unique message even for malicious keys.

In addition, Ed25519 avoids private key memory leakage attacks, and its key clamping mechanism makes the re-use of a Ed25519 key pair for its bi-rationally equivalent X25519 encryption key pair resistant to key leakage attacks via the X25519 key pair.

The baseline for strong authenticity is to use the libsodium Ed25519 signature schem

Strong Confidentiality IND-CCA2

The standard for strong public key encryption (PKE) algorithm is IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack).

A scheme that has IND-CCA2 also has the weaker IND-CCA (Indistinguishability under Chosen Ciphertext Attack) which also has the weaker still IND-CPA (Indistinguishability under Chosen Plaintext Attack).

What IND-CCA2 means is that an adversary can't submit ciphertexts in such a way as to discover the private key used to decipher those texts even when the adversary has access to an oracle that tells the adversary whether or not the ciphertext was a valid ciphertext. In addition, an adversary can't construct a valid ciphertext unless the adversary is aware of the associated plaintext.

https://blog.cryptographyengineering.com/2018/04/21/wonk-post-chosen-ciphertext-security-in-public-key-encryption-part-1/

https://blog.cryptographyengineering.com/2018/07/20/wonk-post-chosen-ciphertext-security-in-public-key-encryption-part-2/)

IND-CCA2 via ECIES, HPKE

Getting IND-CCA2 requires what is called an Integrated Encryption System (IES) that provides a public key encryption scheme. An IES that uses an elliptic curve is called an ECIES.

A notable example of an ECIES that provides a public key encryption scheme with IND-CCA2 is the NaCL/Libsodium *sealed box*.

What is special about an ECIES like NaCL's *sealed box* is that it provides the performance of symmetric encryption but with the end-only viewability of asymmetric public key encryption.

What we mean by end-only viewability is that only the recipient to whom the box is sealed can decrypt the ciphertext. The sender cannot.

The way *sealed box* does this is that it creates a non-interactive Diffie-Hellman (DH) en-de-cryption key using an ephemeral X25519 key pair with the long-term X25519 public key of the recipient.

The sender never sees the ephemeral X25519 private key so it can't reconstruct the DH en-de-decryption key. The *sealed box* includes the ephemeral X25519 public key so that the recipient can reconstruct the DH en-de-cryption key using its own long-term X25519 private key and the provided ephemeral X25519 public key.

The ciphertext is encrypted using symmetric encryption so it's high performant and only the holder of the long-term X25519 private key for the long-term X25519 public used in the *sealed box* to encrypt, can decrypt the ciphertext.

IETF RFC-9180 has generalized ECIES with HPKE (https://www.rfc-editor.org/rfc/rfc9180.html).

RFC-9180 extends basic HPKE with 4 modes of operation in a standardized approach.

The Libsodium sealed box has equivalent properties to RFC-9180 base mode

IND-CCA2 via ECIES, HPKE

Baseline for IND-CCA2 is the Libsodium Crypto Box Seal or Sealed Box.

This uses the X25519 key pairs and the venerable high-performant XSalsa20 stream cipher with the Poly1305 MAC that together provide the AEAD that underlies the sealed box HPKE.

https://libsodium.gitbook.io/doc/advanced/stream_ciphers/xsalsa20

https://en.wikipedia.org/wiki/ChaCha20-Poly1305

HPKE is not Authenticity

IND-CCA2, by itself, is insufficient to provide strong authenticity of the ciphertext.

As section 9.1.1 of RFC-9180 points out, all variants are vulnerable to key-compromise impersonation attacks that may arise from a compromise of the recipient's private key.

This also allows the attacker to purport that the confidential information was meant for the impersonated key pair thus also breaking authenticity.

RFC-9180 suggests that applications that require resistance against key-compromise impersonation should take extra steps to prevent this attack, such as, using a digital signature generated with the sender's private key over the HPKE container, which means signing the *sealed box* (when using Libsodium).

https://eprint.iacr.org/2006/252.pdf

https://www.rfc-editor.org/rfc/rfc9180.html#name-key-compromise-impersonatio

https://www.cryptologie.net/article/372/key-compromise-impersonation-attacks-kci/

https://www.usenix.org/system/files/conference/woot15/woot15-paper-hlauschek.pdf

Best Combined Authenticity and Confidentiality

For combined strong authenticity and confidentiality we need both hybrid public key encryption to the receiver's key pair (with IND-CCA2) and public key signing from the sender's key pair (with SUF-CMA).

There are several ways to combine a cipher text and a signature.

In order to protect against key-compromise impersonation attacks we must sign the encryption with the recipient's public key in plaintext. This is called encrypt-then-sign.

But merely signing the encryption does not provide complete protection against all attacks.

An attacker can strip the signature and resign the ciphertext with the attacker's key but has never seen the plaintext of the cipher. In some circumstances, this might lead the recipient to falsely believe that the sender had knowledge of the plain text when it did not. For that, we must not only bind the recipient's public key to the signature in plaintext but also bind the sender's public key inside the ciphertext.

ESSR (Encrypt Sender Sign Receiver)

An approach that protects against both KCI and sender impersonation of the ciphertext is called ESSR.

https://eprint.iacr.org/2001/079)

https://neilmadden.blog/2018/11/14/public-key-authenticated-encryption-and-why-you-want-it-part-i/

https://neilmadden.blog/2018/11/26/public-key-authenticated-encryption-and-why-you-want-it-part-ii/

https://neilmadden.blog/2018/12/14/public-key-authenticated-encryption-and-why-you-want-it-part-iii/

The properties that protect against key compromise impersonation attacks are called

TUF-PTXT (Third-party UnForgeability of PlainText),

TUF-CTXT (Third-party UnForgeability of CipherText),

RUF-PTXT (Receiver UnForgeability of PlainText),

RUF-CTXT (Receiver UnForgeability of CipherText).

Simply using the encrypt then sign approach provides TUF-PTXT, TUF-CTXT, and RUF-CTXT but not RUF-PTXT.

scheme	TUF-PTXT	TUF-CTXT	RUF-PTXT	RUF-CTXT
Encrypt-then-Sign	X	X		X
ESSR	X	X	X	X

As a result of binding the sender's public key inside the ciphertext and binding the receiver's public key in the enclosing signed plain text an adversary is prevented from forging messages that compromise either authenticity or confidentiality. Thus ESSR provides both strong authenticity and strong confidentiality.

ESSR (Encrypt Sender Sign Receiver)

An approach that protects against both KCI and sender impersonation of the ciphertext is called ESSR.

https://eprint.iacr.org/2001/079)

https://neilmadden.blog/2018/11/14/public-key-authenticated-encryption-and-why-you-want-it-part-i/

https://neilmadden.blog/2018/11/26/public-key-authenticated-encryption-and-why-you-want-it-part-ii/

https://neilmadden.blog/2018/12/14/public-key-authenticated-encryption-and-why-you-want-it-part-iii/

The properties that protect against key compromise impersonation attacks are called

TUF-PTXT (Third-party UnForgeability of PlainText),

TUF-CTXT (Third-party UnForgeability of CipherText),

RUF-PTXT (Receiver UnForgeability of PlainText),

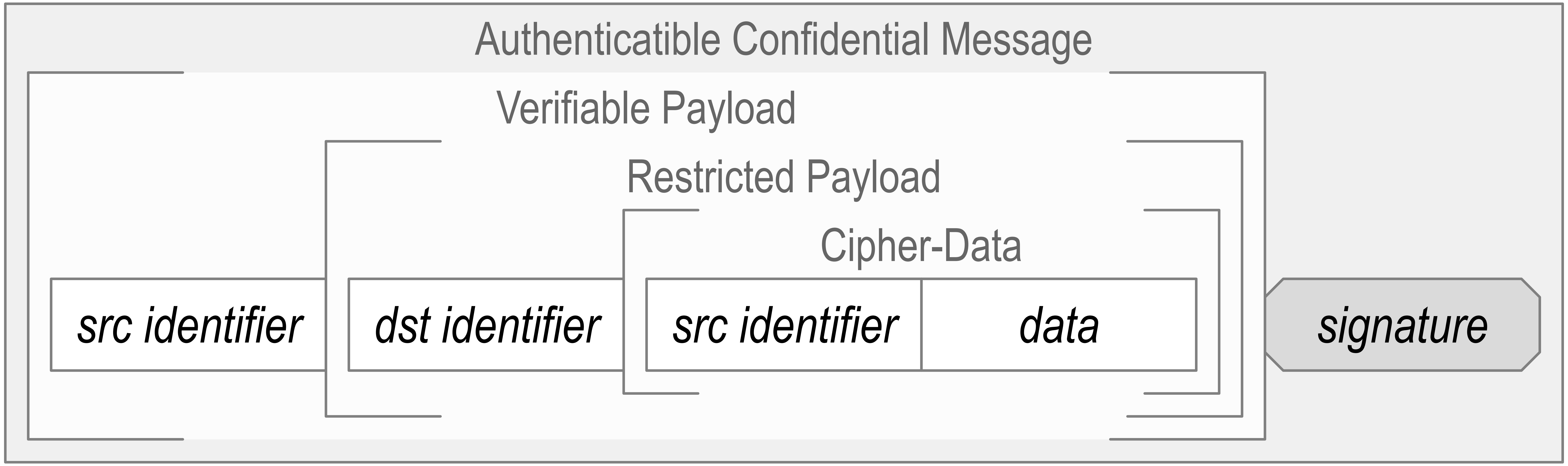
RUF-CTXT (Receiver UnForgeability of CipherText).

Simply using the encrypt then sign approach provides TUF-PTXT, TUF-CTXT, and RUF-CTXT but not RUF-PTXT.

scheme	TUF-PTXT	TUF-CTXT	RUF-PTXT	RUF-CTXT
Encrypt-then-Sign	X	X		X
ESSR	X	X	X	X

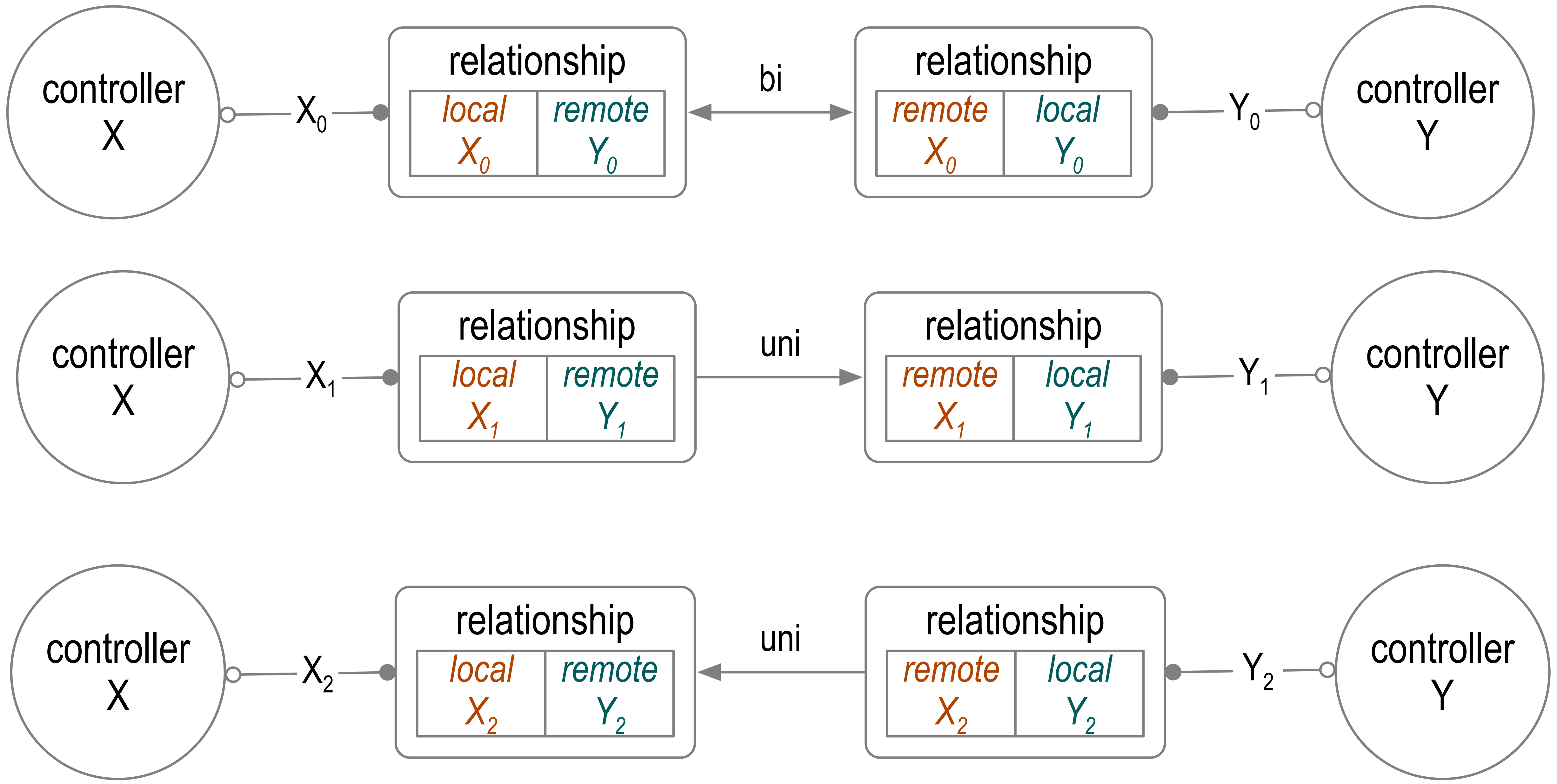
As a result of binding the sender's public key inside the ciphertext and binding the receiver's public key in the enclosing signed plain text an adversary is prevented from forging messages that compromise either authenticity or confidentiality. Thus ESSR provides both strong authenticity and strong confidentiality.

Baseline ESSR Message

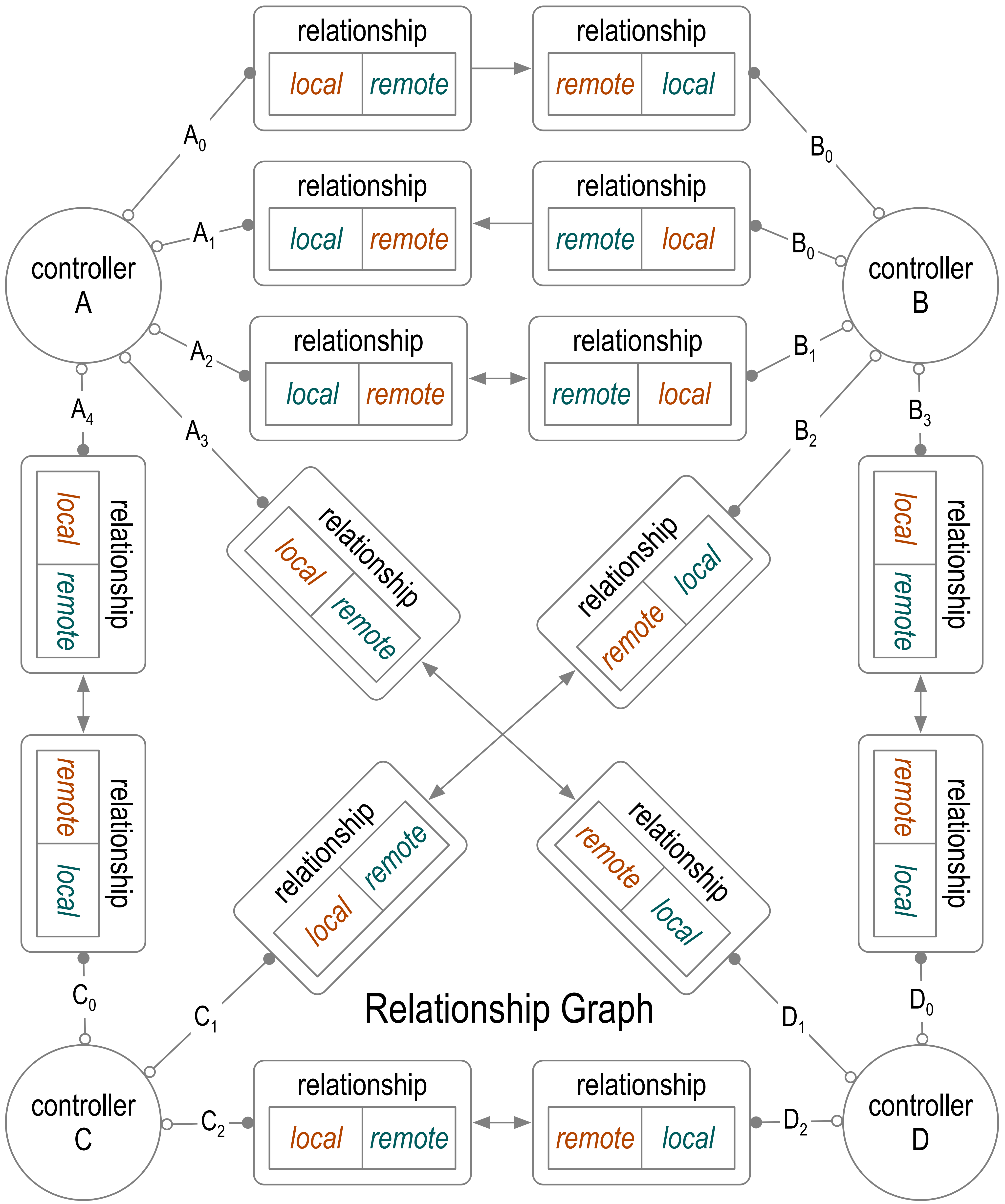


Relationships

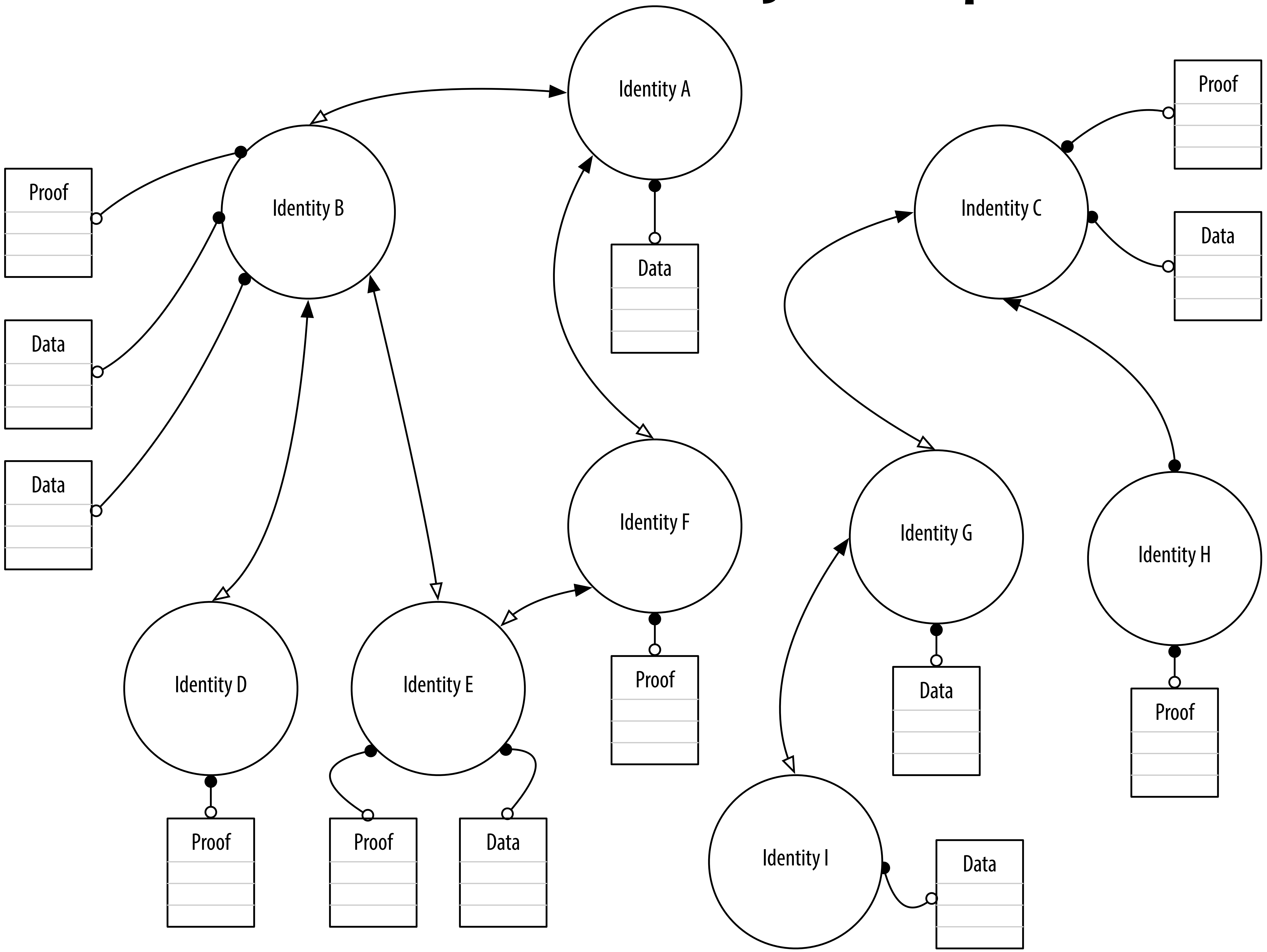
```
(A, <>, B)
(A, ->, B)
(A, <-, B)
```



Relationship Graph (global)



Self-Identity Graph



Relationship graph is the intersection of identity graphs.

Relationship Properties

A ***cryptonym*** is a cryptographically derived pseudonym with at least 128 bits of entropy in the derivation.

An ***AID*** is a cryptonym that is also securely attributable to one or more key pairs.

A ***relationship*** is a pairing of two AIDs, one each from a different *controller*.

*Two different **AIDs** are by themselves uncorrelated in an information-theoretic security sense in that knowledge of one by itself provides no information about the other.*

A ***context*** is a set of events.

*Two **contexts** are disjoint with respect to an AID when that AID appears in one or more events in one set but does not appear in any event in* the *other set.*

A relationship is not a *communication channel*, but the events sent over a communication channel may be a ***context*** for the aids in a ***relationship***.

A ***partition*** is a set of *contexts* with mutually disjoint *relationships*.

*Any set of relationships using **ORIs (One Relationship Identifiers)** may form a partition.*

Any two member *contexts* of a *partition* may be correlatable due to other information associated with those contexts, but the partitioned relationships by themselves provide no correlatable information, i.e., *partitioned relationships* are by themselves not mutually correlatable

An *AID* common to any subset of events within a context provides a *perfectly correlatable* feature across those common events in that context.

Within a context, the *secure attributability* of an AID, together with its *perfect correlatability,* enables secure *reputational trust* (good or bad) in that AID within that context.

Partitions balance the concerns of:

strong authenticity and strong confidentiality within a context with,

sufficiently strong privacy between contexts.

OOB Setup

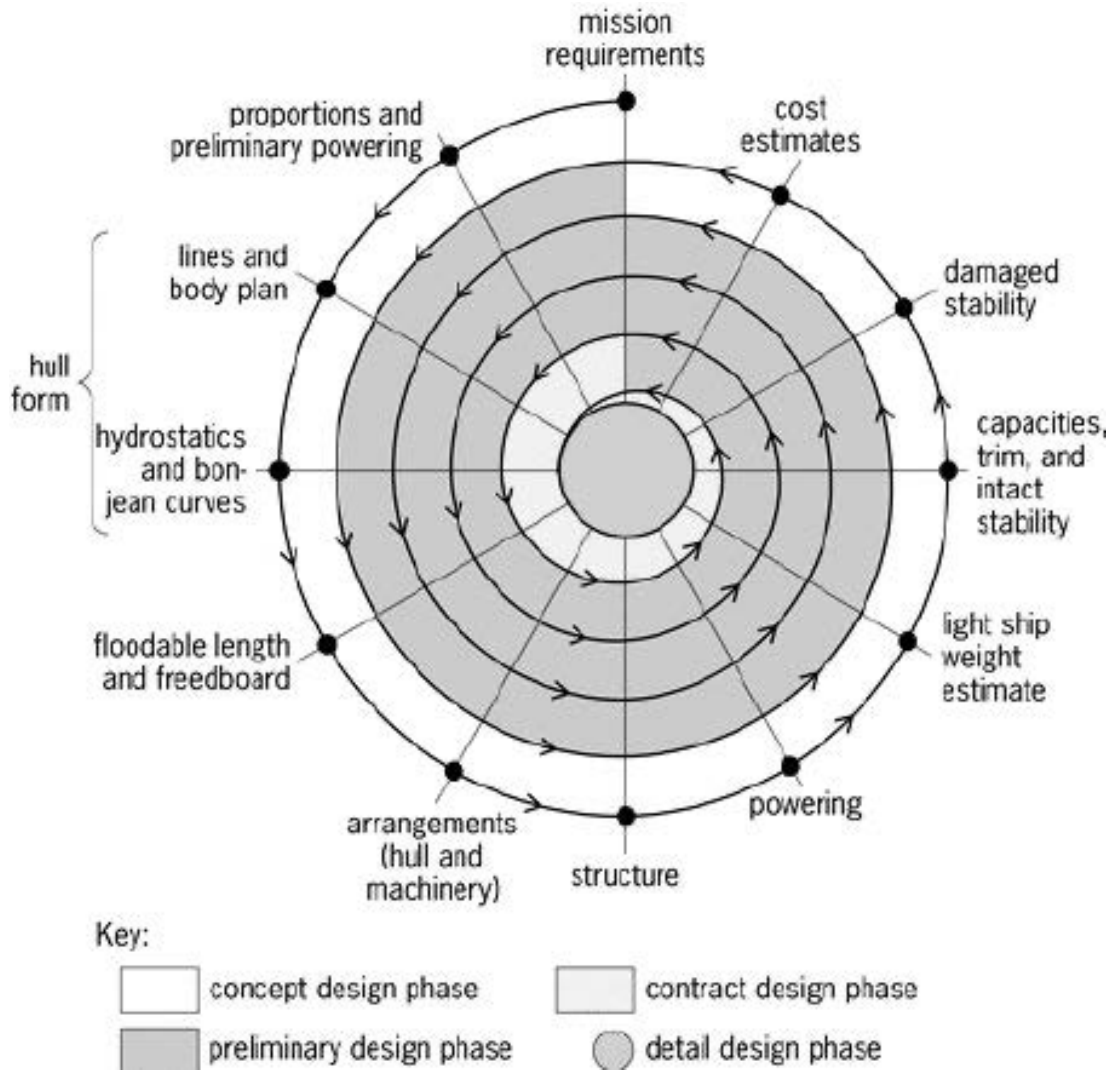
Assume at least one OOBA (out-of-band-authentication) factor to protect from MITM (man-in-the-middle) attack.

OOBA setup also provides protection from cheap pseudonymity.

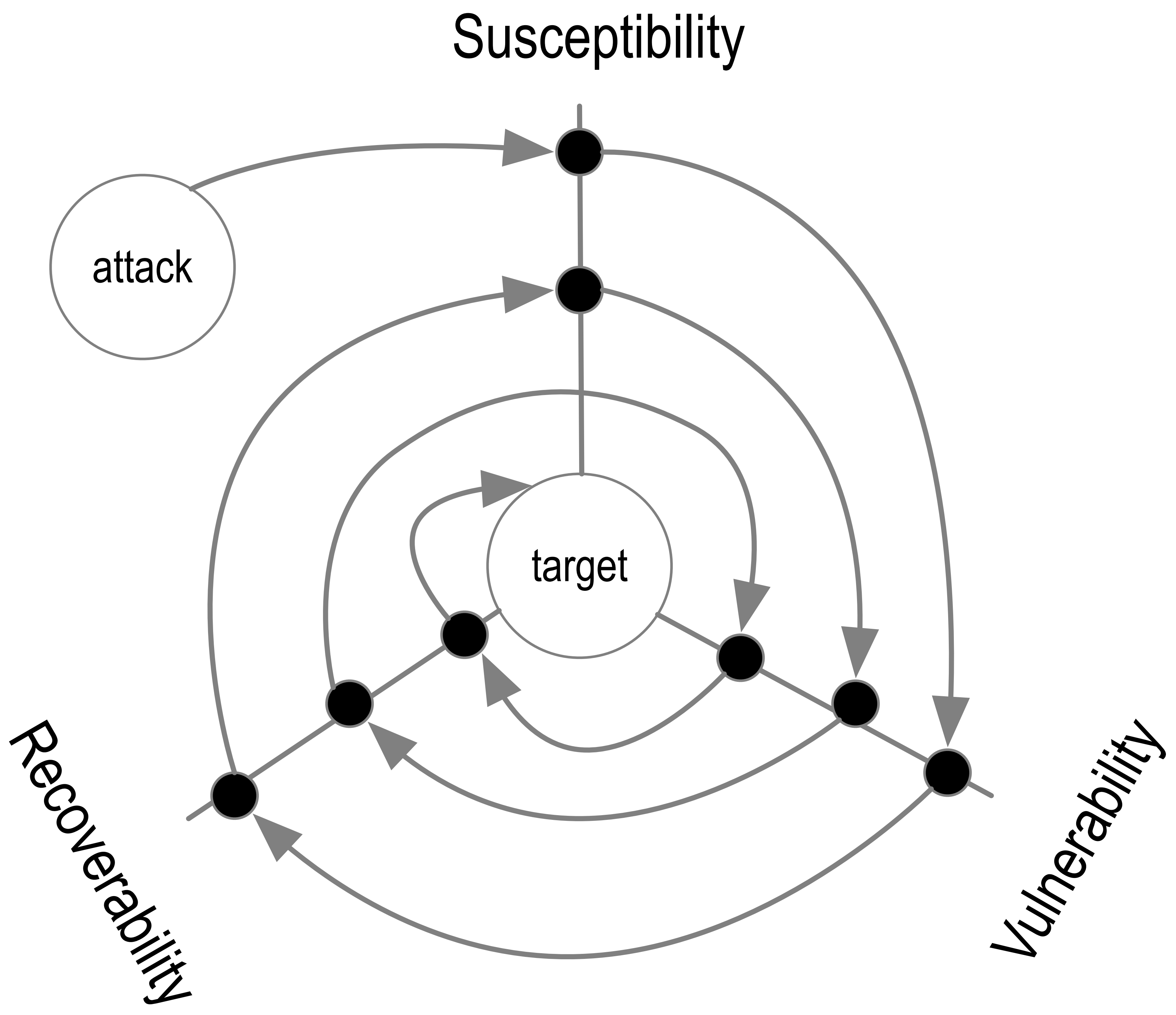
An OOB setup can simultaneously be strongly authentic, confidential, and private.

Multiple Overlay Spiral

Any set of mutually compatible overlays can be flexibly utilized in a spiral fashion
Where one enters, where one exits, where one stops, and how many times around the spiral is application dependent



Naval Architecture Design Spiral



Layered Survivabilty Overlay Spiral

https://www.researchgate.net/publication/273026917_Ship_Design_and_System_Integration/figures?lo=1

Protocol Syntax

AIDs:

X_0, X_1, X_2

Relationships:

$(X_0, <>, Y_0)$

$(X_1, ->, Z_0)$

$(X_2, <-, Y_1)$

Signatures:

$<data>\ X_0$

$<data>\ (X_0, X_1)$

CipherText:

$\{data\}Y_2$

Messages:

$[src\ X_0,\ dst\ Y_0,\ data]$

$<[src\ X_0,\ dst\ Y_0,\ \{src\ X_0,\ data\}Y_0]>X_0$

Interaction Context ID:

$i^0 X_0 Y_0$

Header:

(version, protocol type, packet type, interaction ID, sequence number, ….)

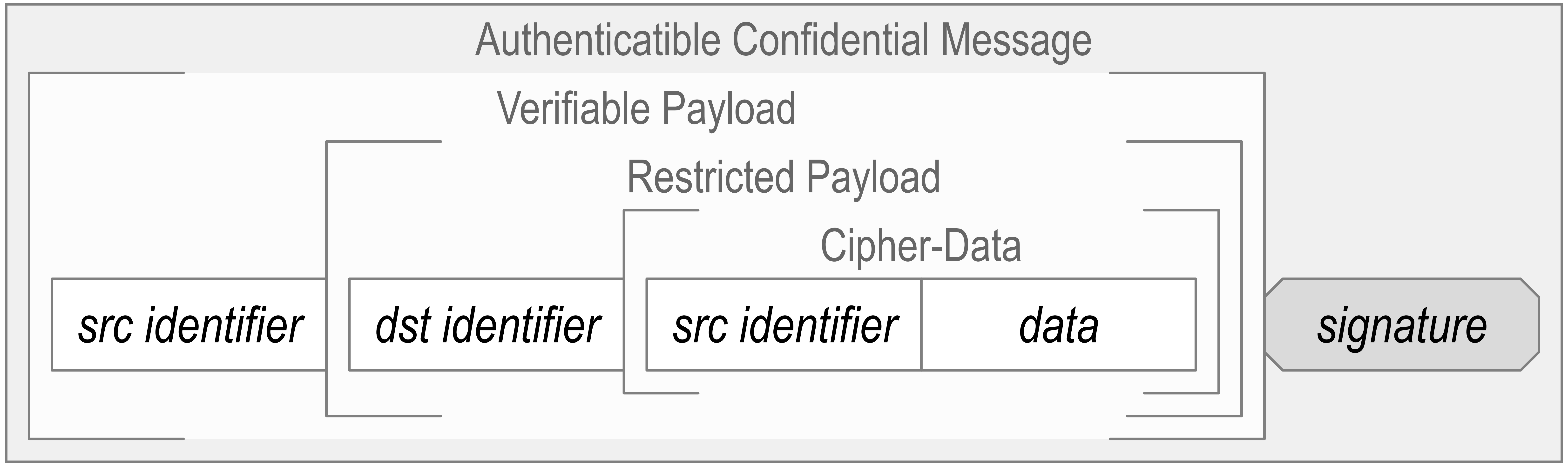
$<[header,\ src\ X_0,\ dst\ Y_0,\ \{src\ X_0,\ data\}Y_0]>X_0$

Transport (IP) Header: (IP addresses are public by nature with inherently correlatable global context)

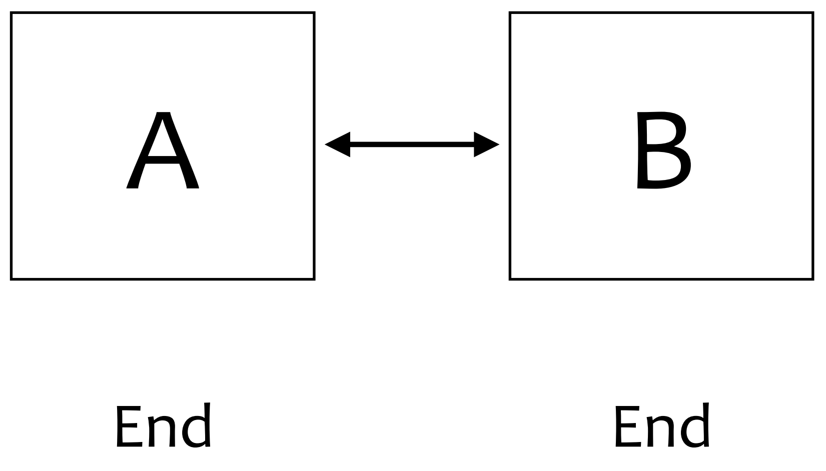
$|src\ ip\ X_0,\ dst\ ip\ Y_0|$

Example:

$|src\ ip\ X_0,\ dst\ ip\ Y_0|<[header,\ src\ X_0,\ dst\ ip\ Y_0,\ dst\ Y_0,\ \{src\ X_0,\ data\}Y_0]>X_0$



Direct Protocol



OOB:

entities: A, B

relationship: $(A_0, <>, B_0)$

service endpoints: $ip\ A_0, ip\ B_0$

IB:

$|src\ ip\ A_0, dst\ ip\ B_0|<[src\ A_0, dst\ B_0, \{src\ A_0, data\}B_0]>A_0$

$|src\ ip\ B_0, dst\ ip\ A_0|<[src\ B_0, dst\ A_0, \{src\ B_0, data\}A_0]>B_0$

Legal Recourse Variant

$|src\ ip\ A_0, dst\ ip\ B_0|<[src\ A_0, dst\ B_0, \{<src\ A_0, data>A_0\}B_0]>A_0$

$|src\ ip\ B_0, dst\ ip\ A_0|<[src\ B_0, dst\ A_0, \{<src\ B_0, data>B_0\}A_0]>B_0$

Correlatable Metadata Identifiers:

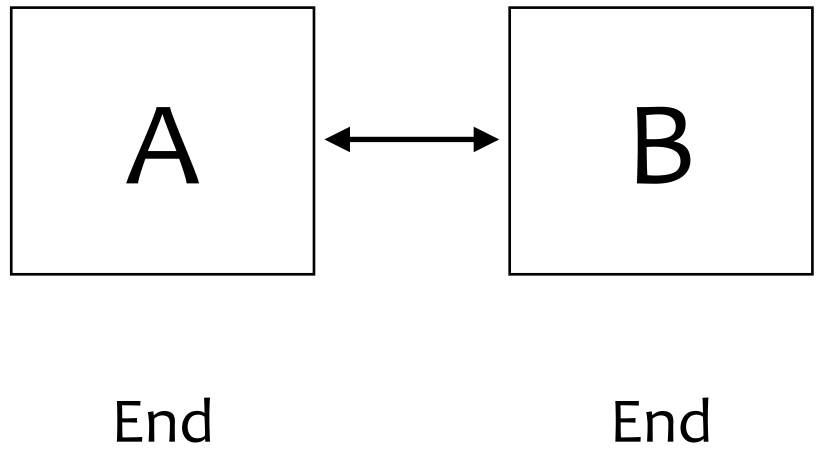
$ip\ A_0, ip\ B_0, A_0, B_0$

Confidential Information:

data

Strongly Authentic and Confidential but not Private

Direct Protocol as Wrapper



OOB:

entities: A, B

relationships: $(A_0, <>, B_0), (A_1, <>, B_1)$

service endpoints: $ip\ A_0, ip\ B_0$

***IB**:*

$|src\ ip\ A_0, dst\ ip\ B_0|<[src\ A_0, dst\ B_0, \{src\ A_0, <[src\ A_1, dst\ B_1, data]>A_1\}B_0]>A_0$

$|src\ ip\ B_0, dst\ ip\ A_0|<[src\ B_0, dst\ A_0, \{src\ B_0, <[src\ B_1, dst\ A_1, data]>B_1\}A_0]>B_0$

Correlatable Metadata Identifiers:

$ip\ A_0, ip\ B_0, A_0, B_0$

Confidential Information:

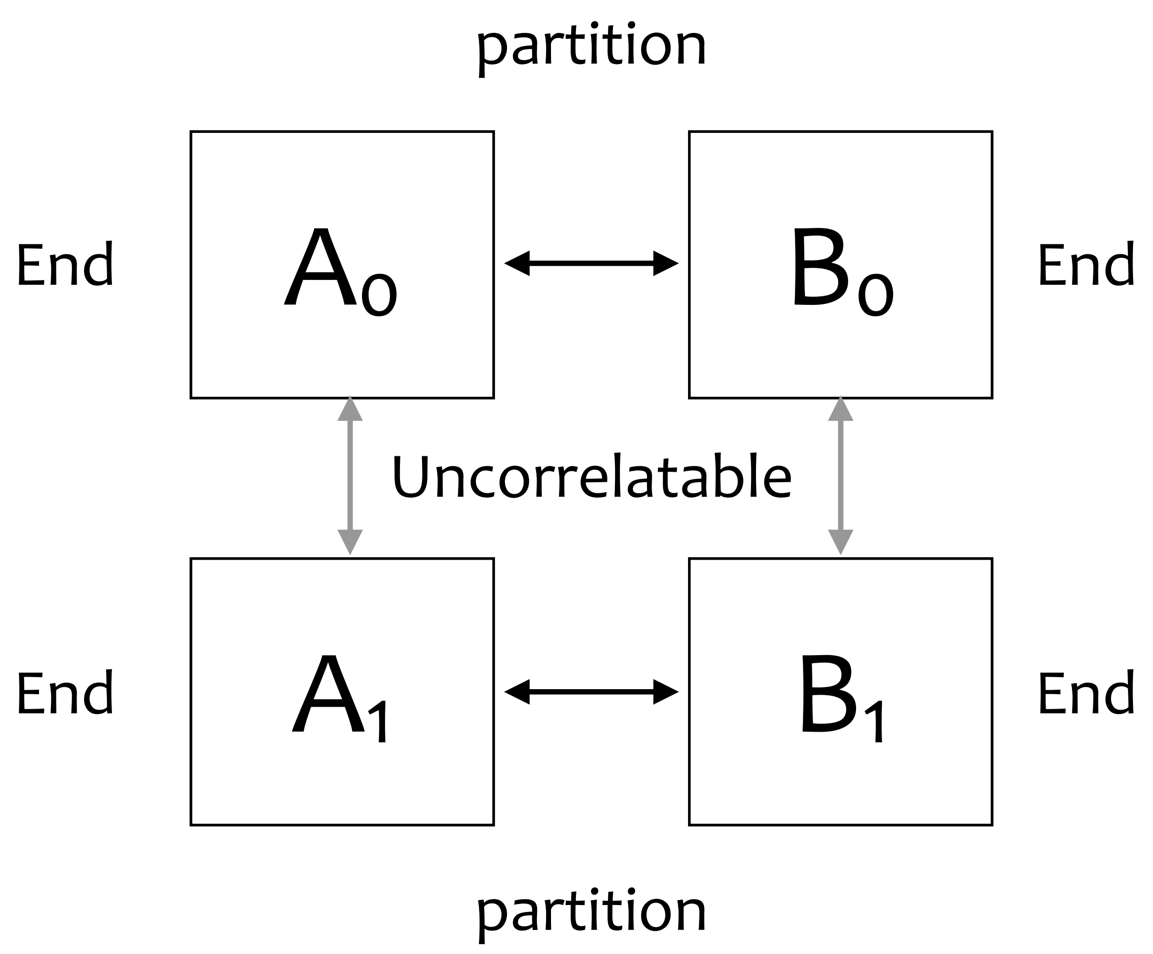
data, A_1, B_1

Private Metadata Identifiers

A_1, B_1

Strongly Authentic and Confidential and Somewhat Private

Relationship Formation Sub-Protocol



OOB:

entities: A, B

relationships: $(A_0, <>, B_0), (A_1, <>, B_1)$,

service endpoints: $ip\ A_0, ip\ B_0$

Interaction Identifier: $i^0A_1B_0$

IB:

$|src\ ip\ A_0, dst\ ip\ B_0|<[src\ A_0, dst\ B_0, \{src\ A_0, <[i^0A_1B_0, A_1]>A_1\}B_0]>A_0$

$|src\ ip\ B_0, dst\ ip\ A_0|<[src\ B_0, dst\ A_0, \{src\ B_0, <[i^0A_1B_0, A_1, B_1]>B_1\}A_0]>B_0$

Correlatable Metadata Identifiers:

$ip\ A_0, ip\ B_0, A_0, B_0$

Confidential Information:

data, A_1, B_1, iA_1B_0

Private Metadata Identifiers

$A_1, B_1, i^0A_1B_0$

Strongly Authentic and Confidential and Somewhat Private

Relationship Formation Sub-Protocol

The relationship formation protocol defined above would allow any pre-existing relationship to bootstrap a new relationship without having to perform yet another OOB setup to exchange identifiers. This could also be used to establish new communications context relationships by adding the exchange of the service endpoint IP addresses in addition to the AIDs for the newly formed relationship. This is all accomplished using a no-compromise secure authentic, confidential, and private exchange between the two parties.

Thus, any given relationship that has been sufficiently authenticated and is therefore reputable (not cheap) can be used to issue the equivalent of a letter of introduction for a new relationship, thereby imbuing the new relationship with reputation. We call this an Out-Of-Band-Introduction (OOBI) because the reputable relationship authentication was established Out-Of-Band with respect to the new relationship.

The original communication context relationship does not leak any correlatable information about the newly formed relationship. The only correlatable information is that each communication context relationship AIDs are correlated with the relationship's IP addresses. To reiterate, There is no correlation to any other relationship, including other communication relationships, unless they both use the same or related IP addresses.

The protocol uses interaction identifiers derived from hashes to link together the messages in the formation interaction. Such hash chaining of multi-message protocols where the messages are also signed makes the set of messages in the interaction a verifiable data structure. This is virtually impervious to attack. Moreover, because cryptographic digests are universally unique, using a digest for the interaction ID of a chain of hash-chained digests that form an interaction chain enables a given interaction to span different communication contexts and still be easy to lookup in an interaction database that is indexed by such digests. Finally, this approach makes it easy to detect replay attacks.

One Shared Intermediary

OOB:

entities: A, B, C

relationships: $(A_1, <>, B_1), (A_2, <>, C_0), (B_2, <>, C_1)$

service endpoints: $ip\ A_2, ip\ B_2, ip\ C_0, ip\ C_1$

C database:

$<[C_0, <[A_2, ip\ A_2]>A_2]>C_0$

$<[C_1, <[B_2, ip\ B_2]>B_2]>C_1$

C has communication relationships with 1000+ other entities

IB:

Hop1 A to C

$|src\ ip\ A_2, dst\ ip\ C_0|<[src\ A_2, dst\ C_0, \{src\ A_2, dst\ C_1, <[src\ A_1, dst\ B_1, \{src\ A_1, data\}B_1]>A_1\ \}C_0]>A_2$

Hop2 C to B

$|src\ ip\ C_1, dst\ ip\ B_2|<[src\ C_1, dst\ B_2, \{src\ C_1, <[src\ A_1, dst\ B_1, \{src\ A_1, data\}B_1]>A_1\ \}B_2]>C_1$

Correlatable Metadata Identifiers:

$(ip\ A_2, ip\ C_{0,} A_{2,} C_0)$

$(ip\ B_2, ip\ C_{1, B2,} C_1)$

Confidential Information:

data, $A_1, B_{1,}$

Private Metadata Identifiers

A_1, B_1

Strongly Authentic and Confidential and Mostly Private

One Shared Intermediary

The AIDS in $(A_1, <>, B_1)$ are never stored on disk by C. They are only ever in memory. This means that an attacker who compromises the disk storage of C cannot leak $(A_1, <>, B_1)$.

An attack on C's protected memory processes is much more difficult than an attack on C's disk storage. This is more than sufficient to protect against 3rd party correlation for advertising aggregation.

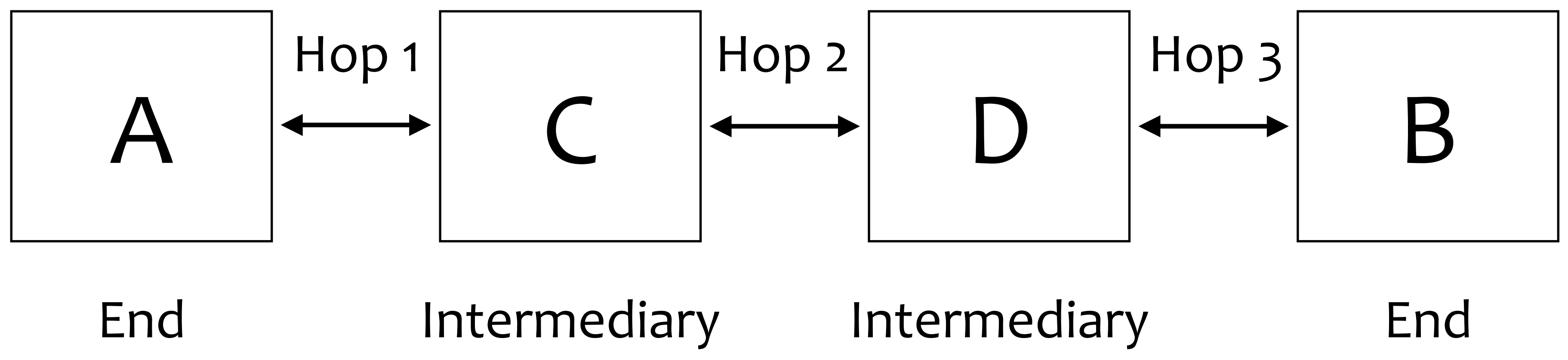
A does not need to know the B side of B's relationship with C, and B does not need to know the A side of A's relationship with C. So neither can leak that information. An attacker has to get that by attacking C, not either A or B.

Thus A and B can isolated their independent hop-wise communications contexts with C from their joint end-wise routing context. The three contexts form a partition with respect to 3rd party correlatability of the AIDs.

The primary limitations of this approach are as follows:

- Both A and B must trust C.
- The ISP of C has access to both the source and destination IPs of all C's packets. With some extra work, the ISP could correlate observable statistics (but not AIDs) about the packets, such as time-of-arrival and time-of-departure, packet size, packet type, protocol types, etc.

Non Shared Intermediaries



OOB:

entities: A, B, C, D

relationships: (A_1, <>, B_1), (A_2, <>, C_0), (B_2, <>, D_0), (C_2, <>, D_2)

service endpoints: ip A_2, ip B_2, ip C_0, ip D_0, ip C2, ip D_2

C database: <[C_0,<[A_2, ip A_2]>A_2]>C_0 <[A_2, D_2, ip D_2]>A_2

D database: <[D_0,<[B_2, ip B_2]>B_2]>D_0 <[B_2, C_2, ip C_2]>B_2

C and D each have communication relationships with 1000+ other entities

IB:

Hop1 A to C

|src ip A_2, dst ip C_0|<[src A_2, dst C_0, {src A_2, dst D_2, dst D_0, <[src A_1, dst B_1, {src A_1, data}B_1]>A_1}C_0]>A_2

Hop2 C to D

|src ip C_2, dst ip D_2|<[src C_2, dst D_2, {src C_2, dst D_0, <[src A_1, dst B_1, {src A_1, data}B_1]>A_1}D_2]>C_2

Hop3 D to B

|src ip D_0, dst ip B_2|<[src D_0, dst B_2, {src D_0, <[src A_1, dst B_1, {src A_1, data}B_1]>A_1}B_2]>D_0

Correlatable Metadata Identifiers:

(ip A_2, ip C_0, A_2, C_0, D_2, D_0)

(ip B_2, ip D_0, B_2, D_0, C_2, C_0)

Confidential Information:

data, A_1, B_1, A_2, B_2

Private Metadata Identifiers

A_1, B_1, A_2, B_2

Strongly Authentic and Confidential and Very Private

Non Shared Intermediaries

All any 3rd party ISP sees is that A_2 has a relationship with C and B_2 has a relationship with D but can't correlate those relationships to (A1, <>, B1) given sufficient herd privacy of C's and D's relationships with others.

A and B both trust that C and D do not leak (A1, <>, B1).

The AIDS in (A1, <>, B1) are never stored on disk by either C or D. They are only ever in memory. This means that an attacker who compromises the disk storage of C or D cannot leak (A1, <>, B1). An attack on C's or D's protected memory processes is much more difficult than an attack on C's or D's disk storage.

A does not need to know the B side of B's relationship with D, and B does not need to know the A side of A's relationship with C. So neither can leak that information.

An attack on C's disk does not expose that A has a relationship with any of D's relationships because the farside destination is only exposed in memory. Likewise, an attack on D's disk does not expose that B has any relationships with A because the farside destination is only exposed in memory.

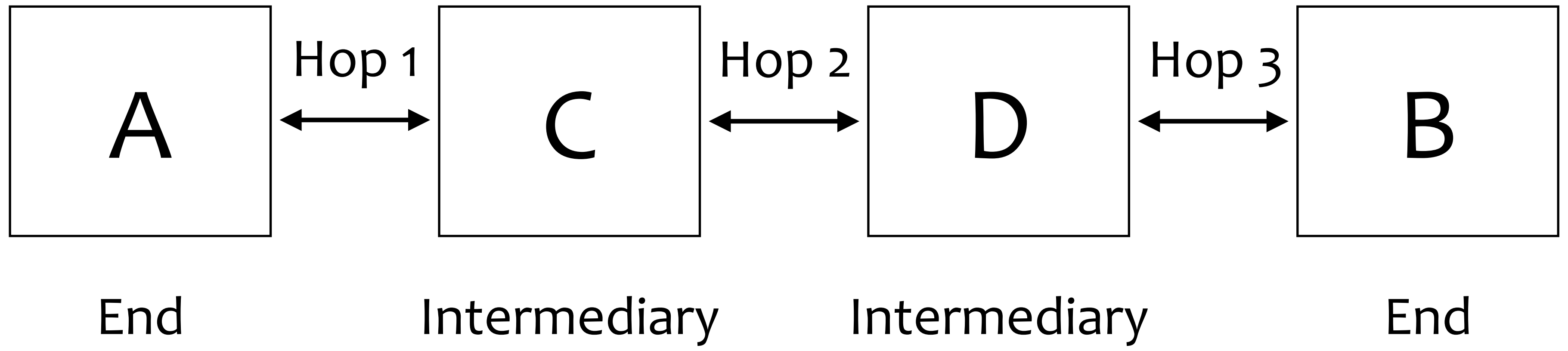
This approach is fully zero-trust because all table lookups by C and D are signed at rest, so an attacker can't misdirect traffic between the two or between their associated edge relationships.

A, B, C, and D have isolated their independent hop-wise communication contexts with each other from the A and B joint end-wise context (A1, <>, B1). The end-wise relationship provides both an end-to-end routing context at the AID level and an end-to-end interaction context. These four contexts (independent hop-wise and joint end-wise) are mutually partitioned wrt 3rd party correlation.

We can conclude that we can have secure authenticity, confidentiality, and privacy (identifier correlation), as well as DDOS protection.

The only OOB setups are one-time setups between A and B, A and C, and B and D.

Non Shared Intermediaries as Wrapper



OOB:

entities: A, B, C, D

relationships: $(A_3, <>, B_3)\ (A_1, <>, B_1), (A_2, <>, C_0), (B_2, <>, D_0), (C_2, <>, D_2)$

service endpoints: $\text{ip } A_2, \text{ip } B_2, \text{ip } C_0, \text{ip } D_{0,}\ \text{ip } C2, \text{ip } D_2$

C database: $<[C_0, <[A_2, \text{ip } A_2]>A_2]>C_0\quad <[A_2, D_2, \text{ip } D_2]>A_2$ *, C has communication relationship with 1000+ other entities*

D database: $<[D_0, <[B_2, \text{ip } B_2]>B_2]>D_0\quad <[B_2, C_2, \text{ip } C_2]>B_2$*, D has communication relationship with 1000+ other entities*

Interaction Identifier: $i^0A_3B_3$

IB:

Hop1 A to C

$|\text{src ip } A_2, \text{dst ip } C_0|<[\text{src } A_2, \text{dst } C_0, \{\text{src } A_2, \text{dst } D_2, \text{dst } D_0, <[\text{src } A_1, \text{dst } B_1,\ \{\text{src } A_1, \mathbf{<[src\ A_3, dst\ B_3,\ i^0A_3B_3, data\ ]>A_3}\}B_1]>A_1\}C_0]>A_2$

Hop1 A to C Variant

$|\text{src ip } A_2, \text{dst ip } C_0|<[\text{src } A_2, \text{dst } C_0, \{\text{src } A_2, \text{dst } D_2, \text{dst } D_0, <[\text{src } A_1, \text{dst } B_1,\ \{\text{src } A_1, \mathbf{<[src\ A_3, dst\ B_3,\ \{src\ A_3, i^0A_3B_3, data\}B_3\ ]>A_3}\}B_1]>A_1\}C_0]>A_2$

Correlatable Metadata Identifiers:

$(\text{ip } A_2, \text{ip } C_{0,} A_{2,} C_0, D_{2,} D_0)$

$(\text{ip } B_2, \text{ip } D_0, B_{2,} D_{0,} C_2, C_0)$

Confidential Information:

data, $A_1, B_{1,} A_2, B_2, \mathbf{A_3, B_{3,} i^0A_3B_3}$

Private Metadata Identifiers

$A_1, B_{1,} A_2, B_{2,} \mathbf{A_3, B_{3,} i^0A_3B_3}$

Strongly Authentic and Confidential and Private

Non Shared Intermediaries as Wrapper

This approach inherits all the properties of Non-Shared intermediaries but with the following additions:

C and D can not leak (A3, <>, B3)

The aids in (A3, <>, B3) are never viewed by C or D.

A, B, C, and D have isolated their independent hop-wise communication contexts with each other from the A and B joint end-wise context (A1, <>, B1) and from the end-wise interaction context (A3, <>, B3) .

The end-wise relationship (A1, <>, B1) only provides a generic end-to-end routing context at the AID level

The end-wise relationship (A3, <>, B3) provides an end-to-end interaction context. These five contexts (independent hop-wise and joint end-wise) are mutually partitioned wrt 3rd party correlation.

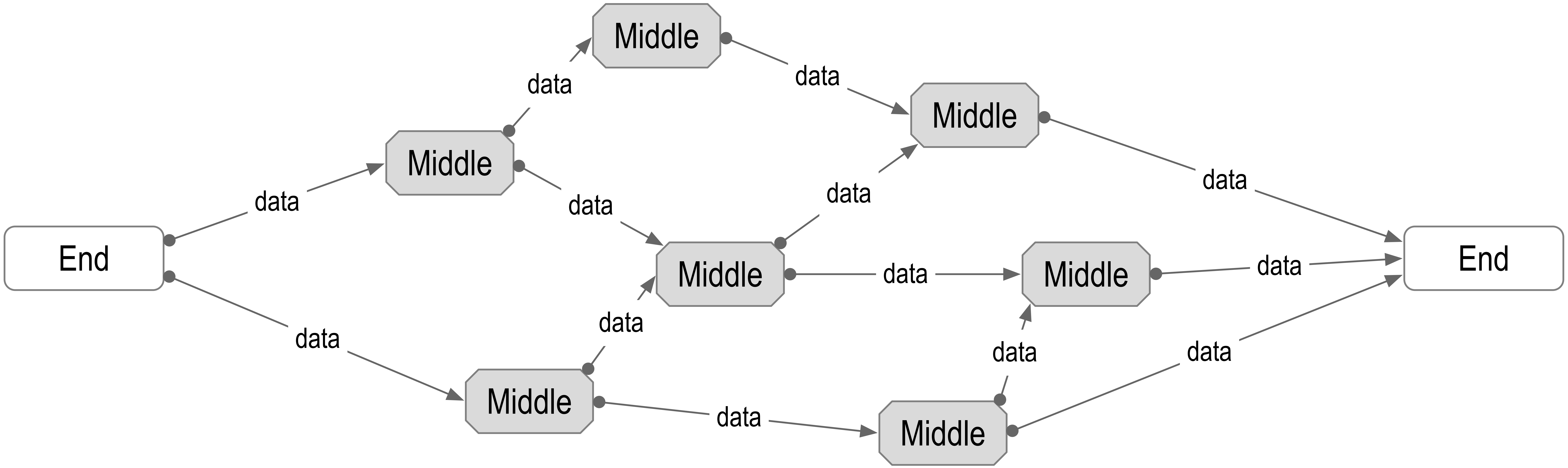
The interaction context (A3, <>, B3) is also partitioned with respect to C and D.

We can conclude that we can have secure authenticity, confidentiality, and privacy (identifier correlation), as well as DDOS protection.

The only OOB setups are one-time setups between A and B, A and C, and B and D.

Dual End Verifiability and End-Only Viewability

End-to-End Verifiability *of Authenticity*
Only-at-End Viewability via Confidentiality



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

End only Viewability: one-data, one-where, one-time by one-body

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

Zero-Trust-Computing

Its much easier to protect one's private keys than to protect all internet infrastructure

Strong End-Only-Viewable Confidentiality

Use the 3-party model where:

1st party is the sender,

2nd party is the intended receiver

3rd party is any unintended receiver.

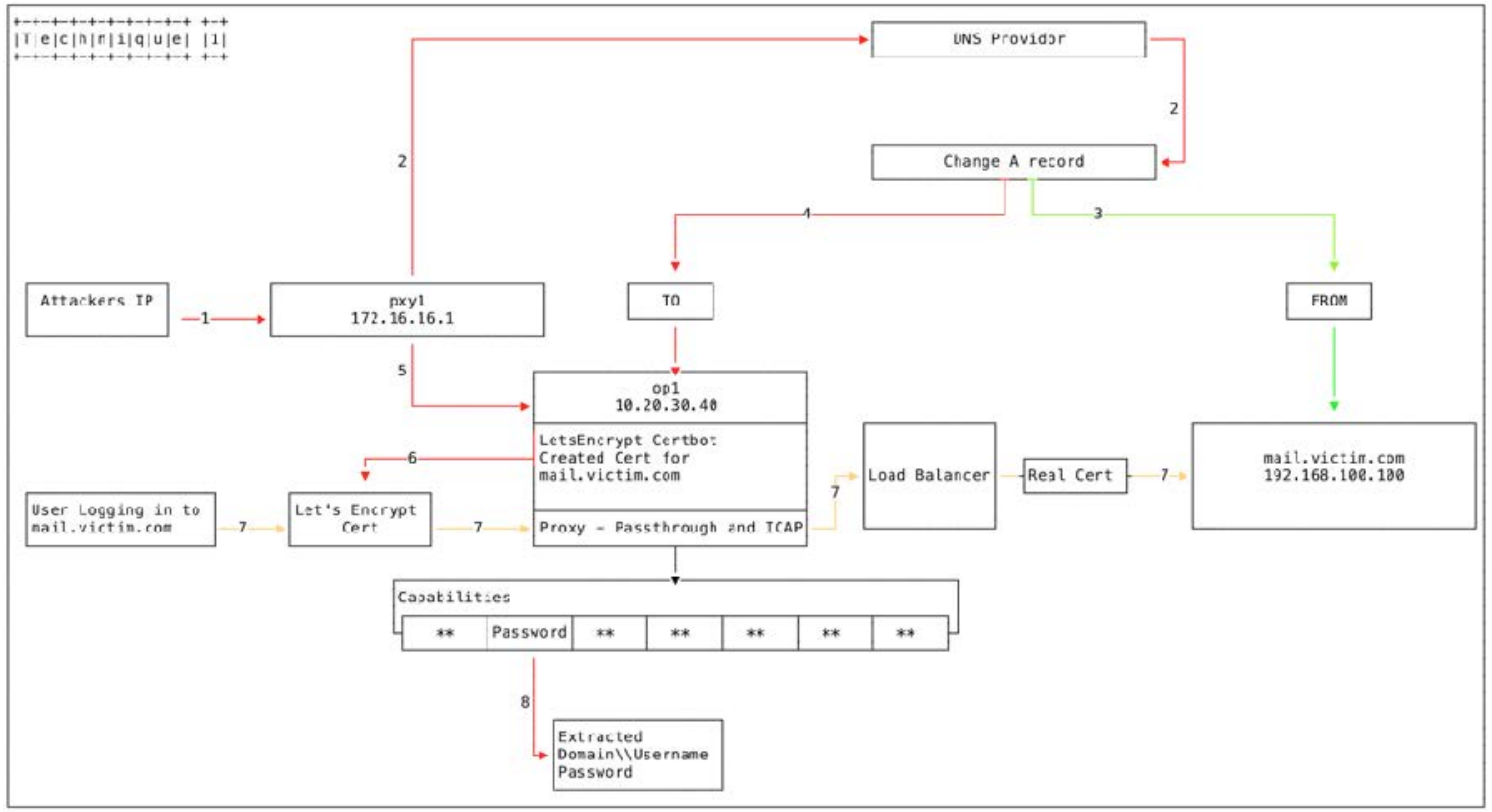
A system with strong end-only viewable confidentiality may have the following properties:

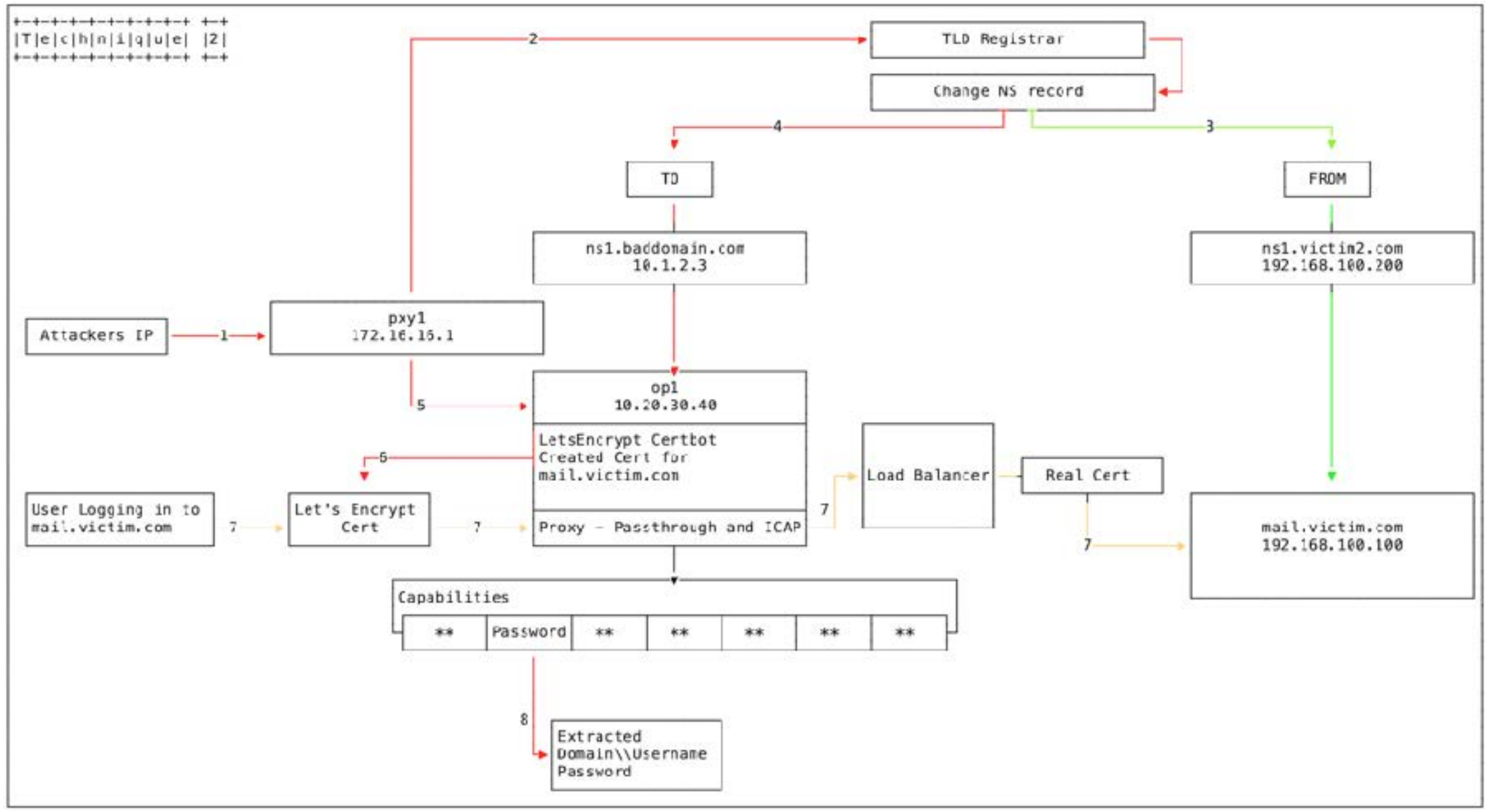
- 3rd party non-viewability
- 1st party non-viewability (this protects 1st party from liability wrt to 2nd party and protects 2nd party from exploit by 1st party) (see appendix for a more detailed description of this property)
- 2nd party partition-ability by 1st party
- Detectable leakage (2nd party to 3rd party)
- Detectable collusion of 2nd party against 1st party (2nd party with 2nd party, or 2nd party with 3rd party)
- Detectable collusion of 1st party against 2nd party (1st party with another 1st party relative to same 2nd party or 1st party with 3rd party)

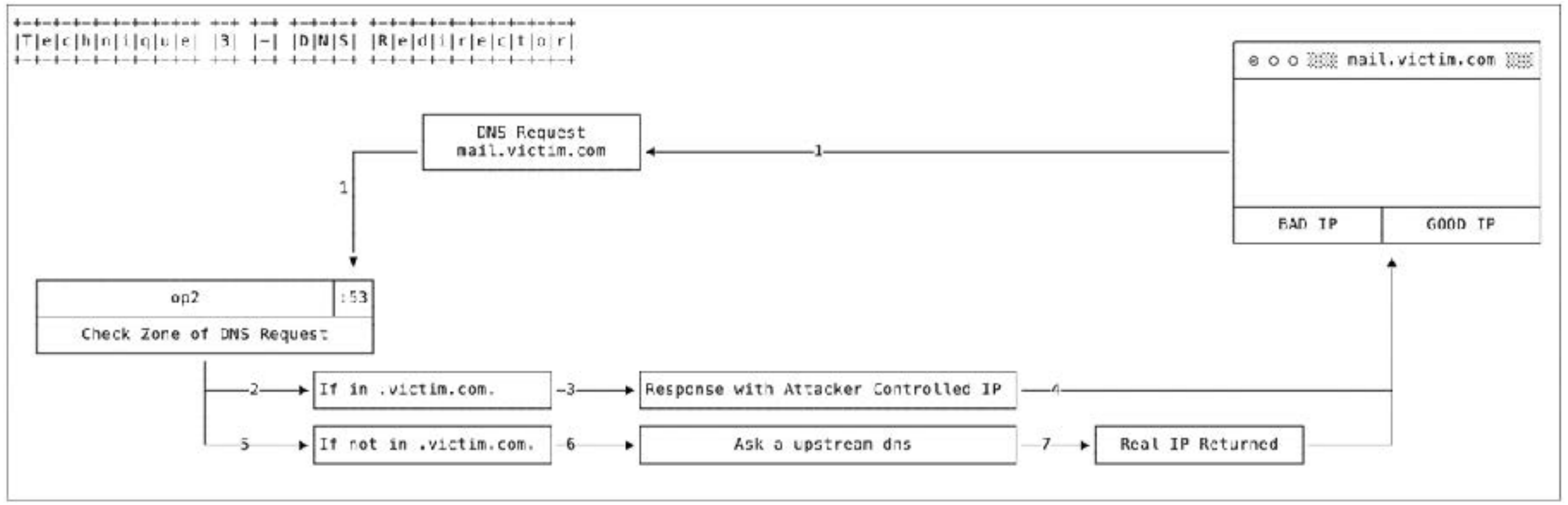
DNS Hijacking

DNS hijacking uses clever tricks that enable 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/





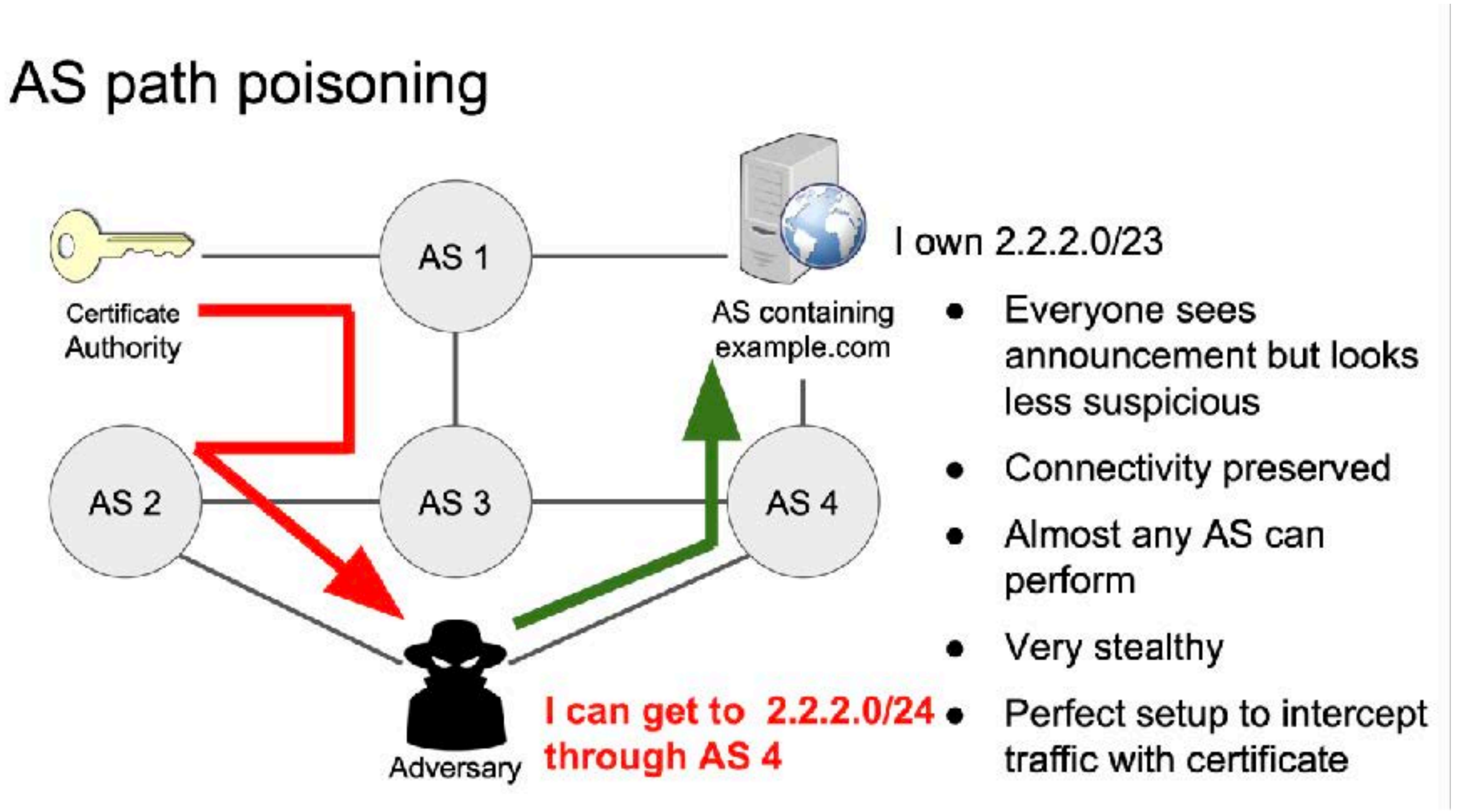


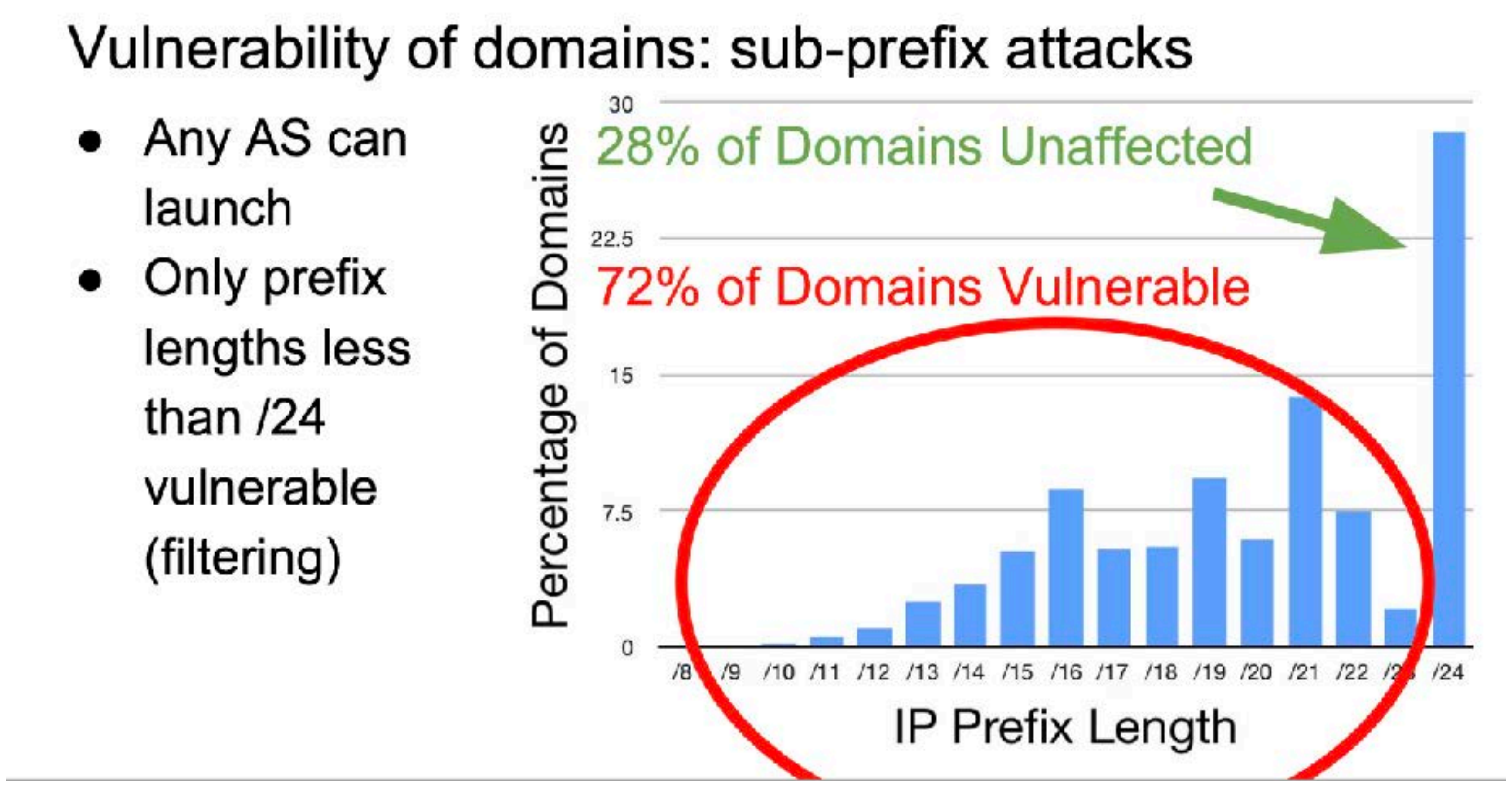
BGP Hijacking: AS Path Poisoning

Spoofing domain verification process from CA enables 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

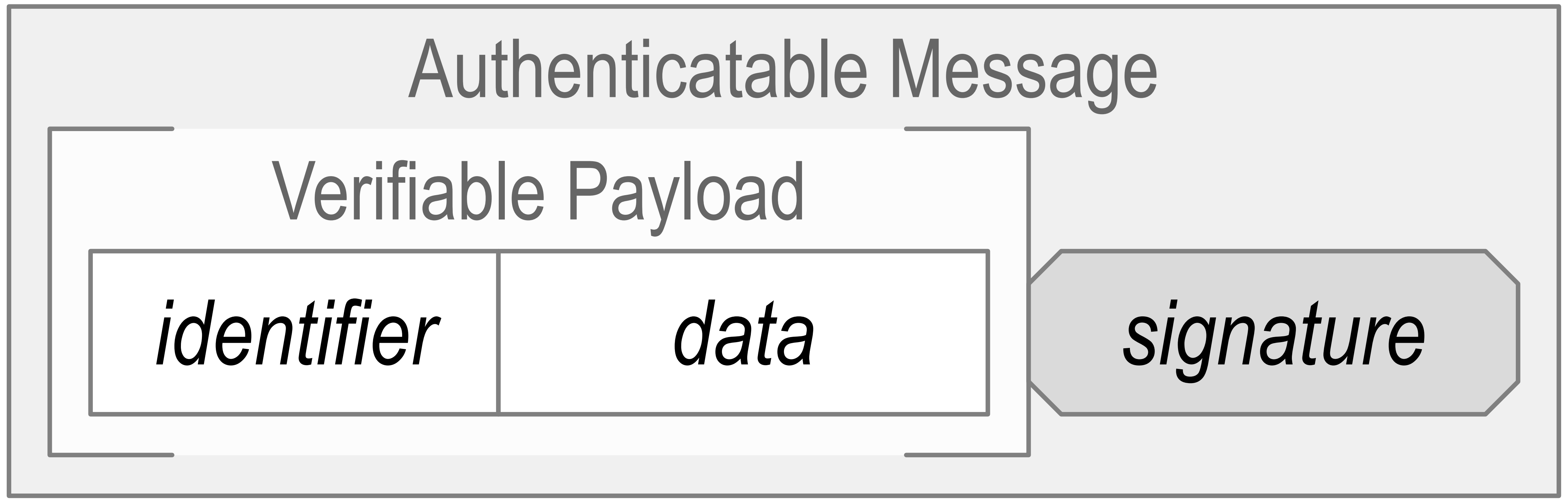
Gavrichenkov, A., “Breaking HTTPS with BGP Hijacking,” BlackHat, 2015 https://www.blackhat.com/docs/us-15/materials/us-15-Gavrichenkov-Breaking-HTTPS-With-BGP-Hijacking-wp.pdf

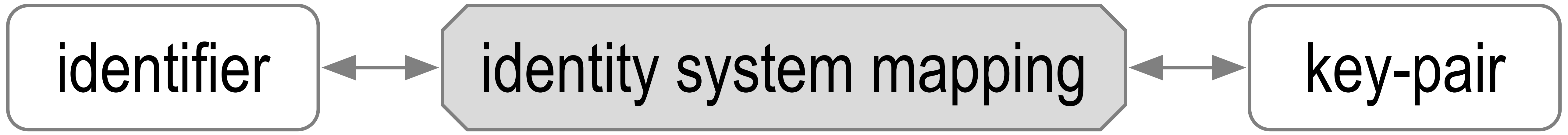




Identity (-ifier) System Security Overlay

Establish authenticity of IP packet's message payload.

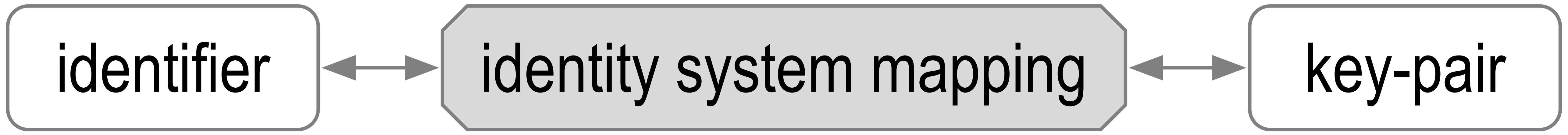




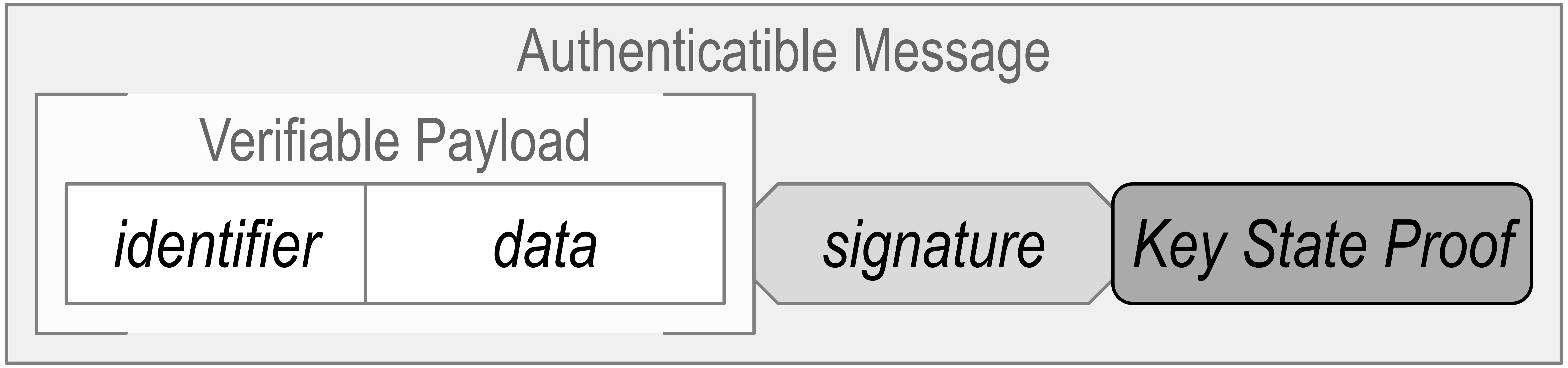
The overlay's security is contingent on the mapping's security.

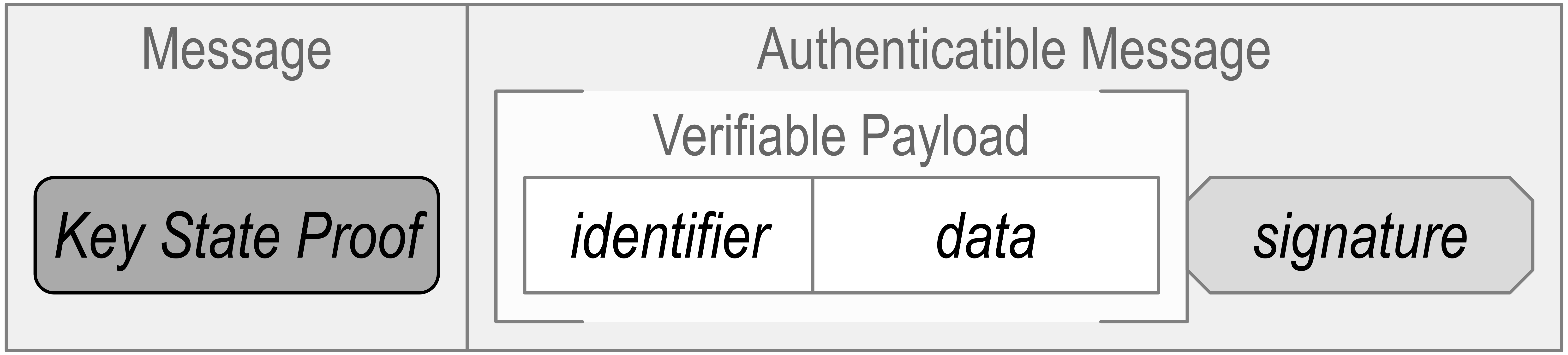
Identity (-ifier) System Security Overlay

persistent (transferable) mapping = verifiable data structure of key state changes



Establish authenticity of IP packet's message payload.

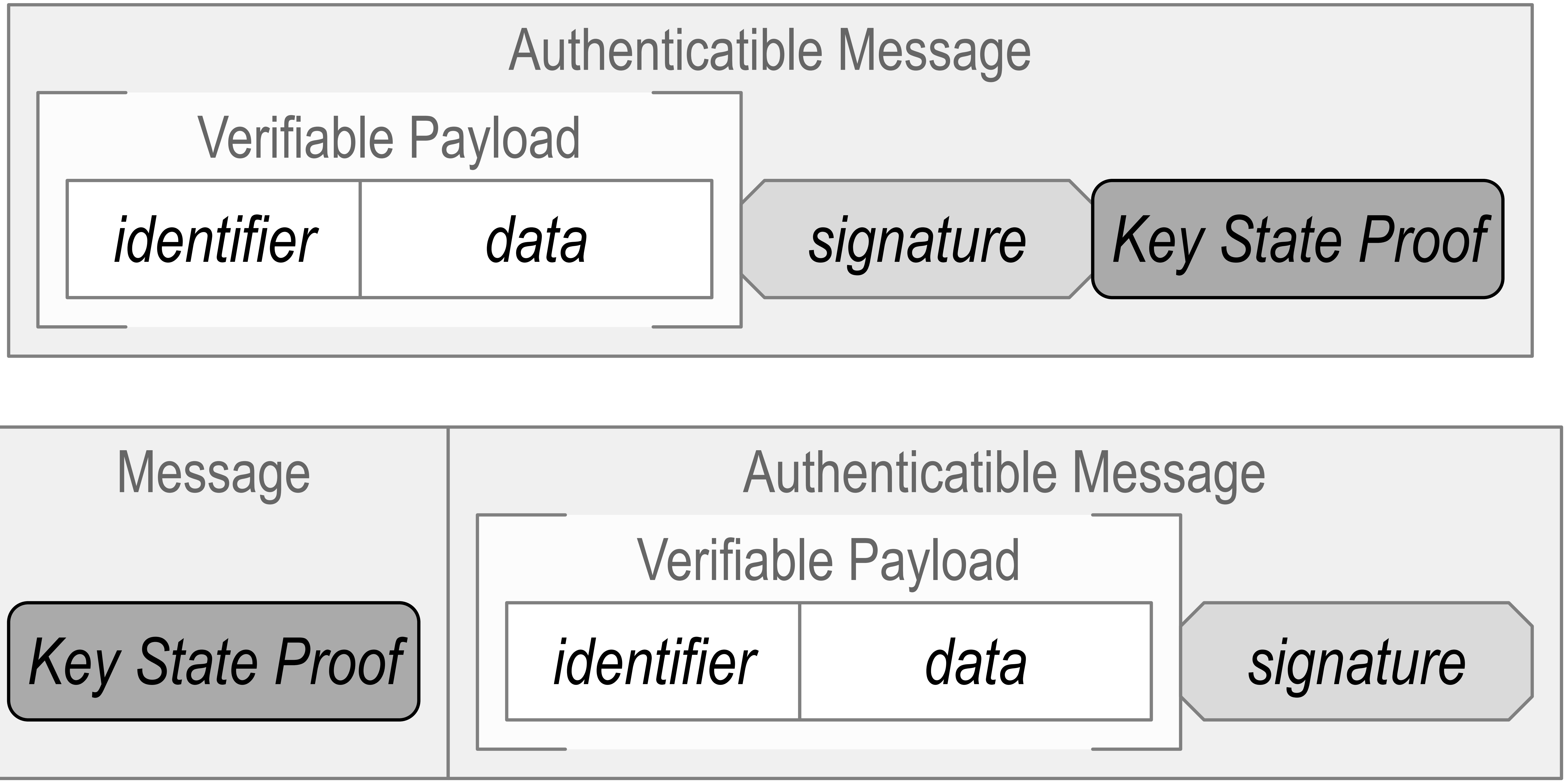




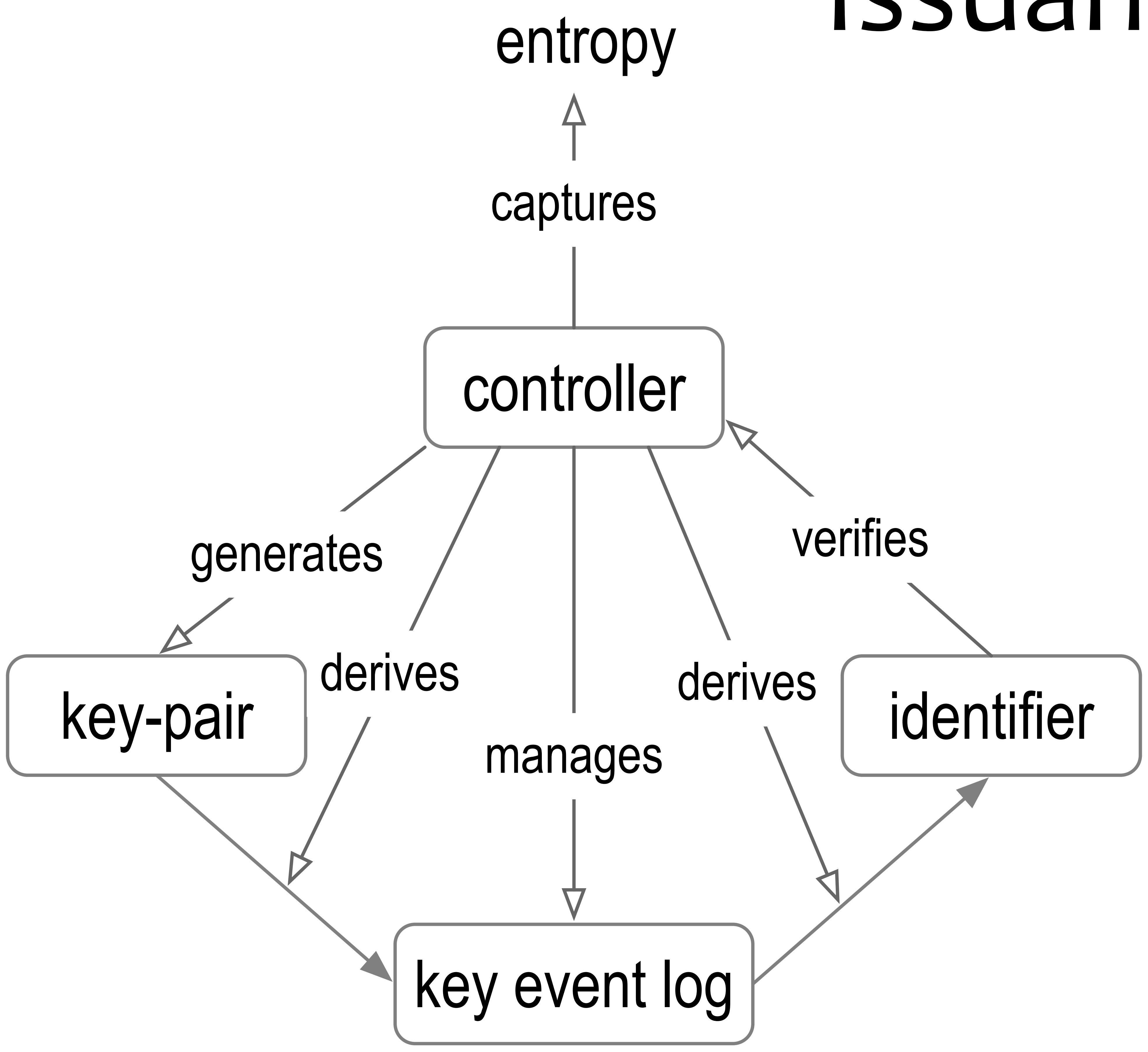
Identity (-ifier) System Security Overlay

persistent (transferable) mapping = verifiable data structure of key state changes

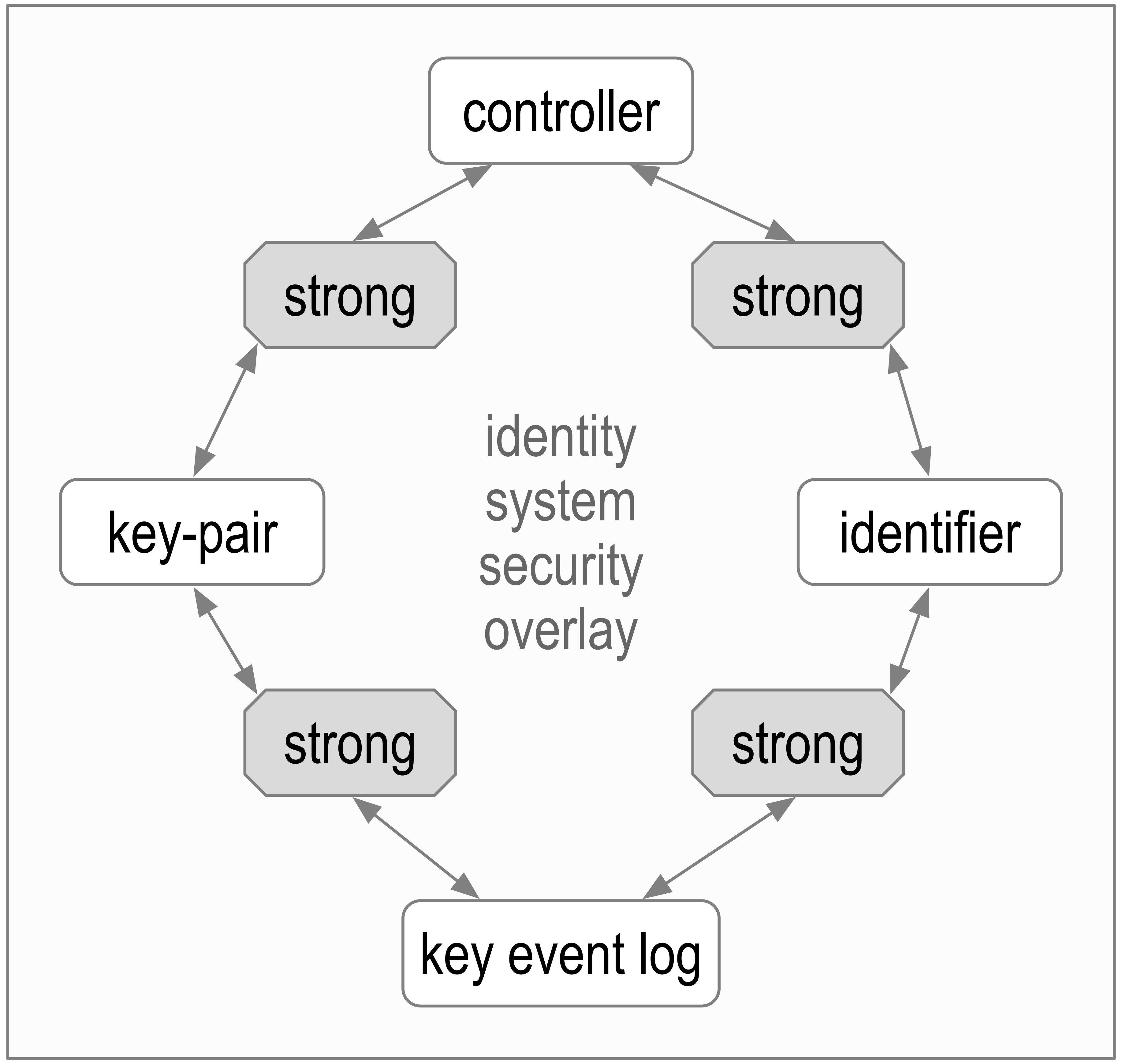
Establish authenticity of IP packet's message payload.



Autonomic Identifier (AID) (Persistent): Issuance and Binding



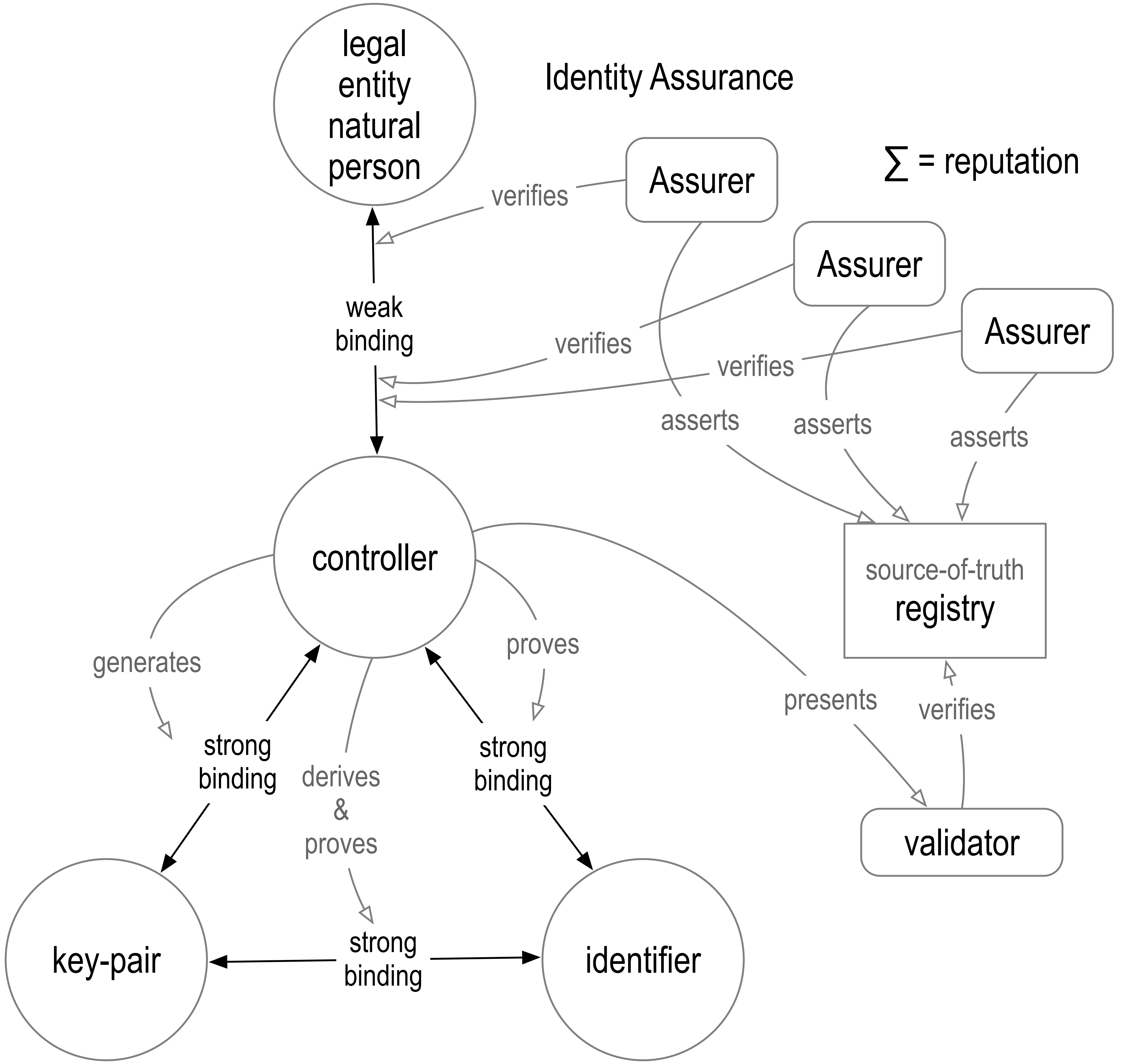
autonomic, self-managing



Autonomic Identifier Issuance Tetrad

cryptographic root-of-trust & verifiable persistent control

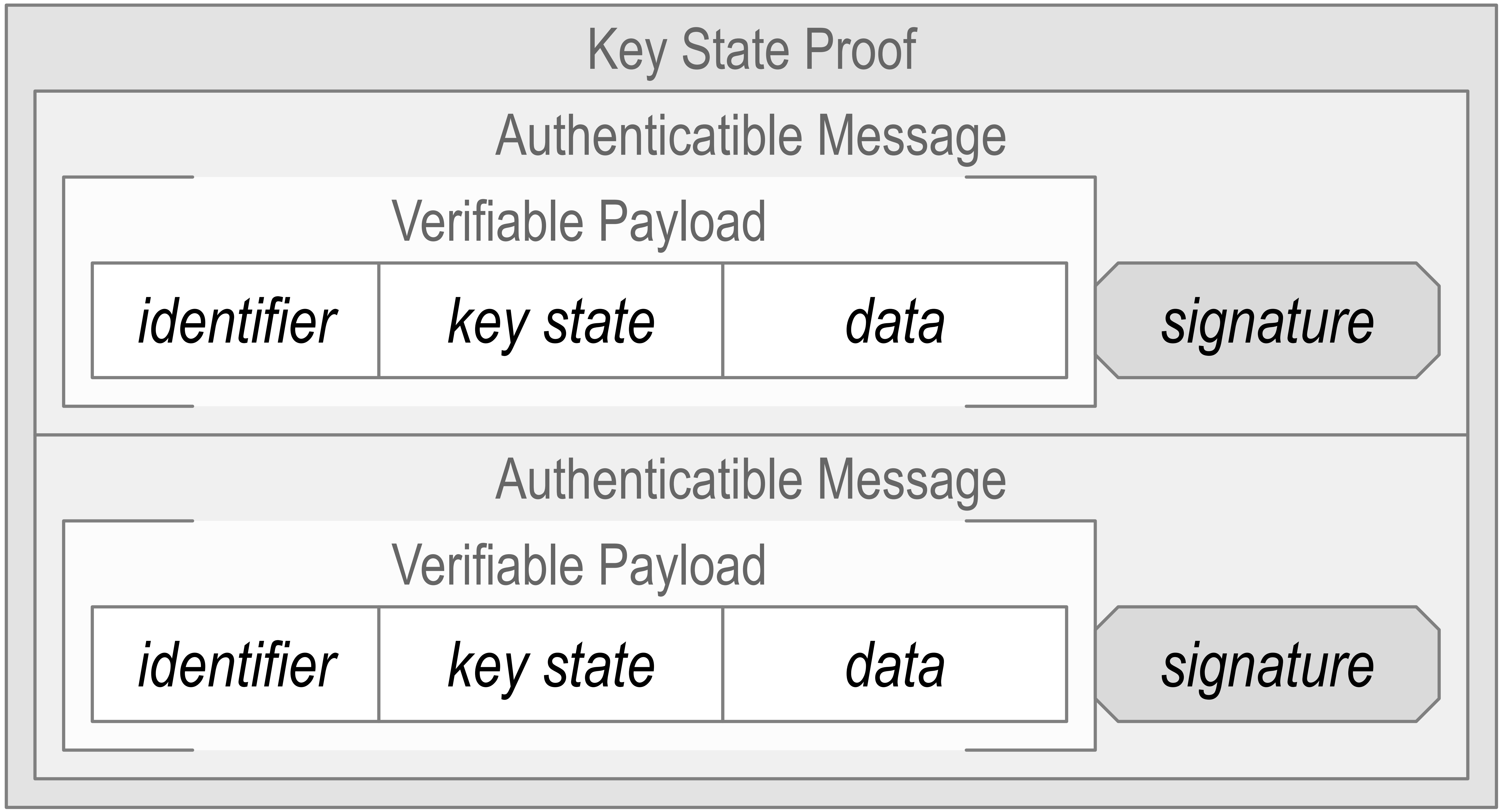
Identity Assurance and Reputation



Relatively weak binding reinforced by multiple bindings = reputation

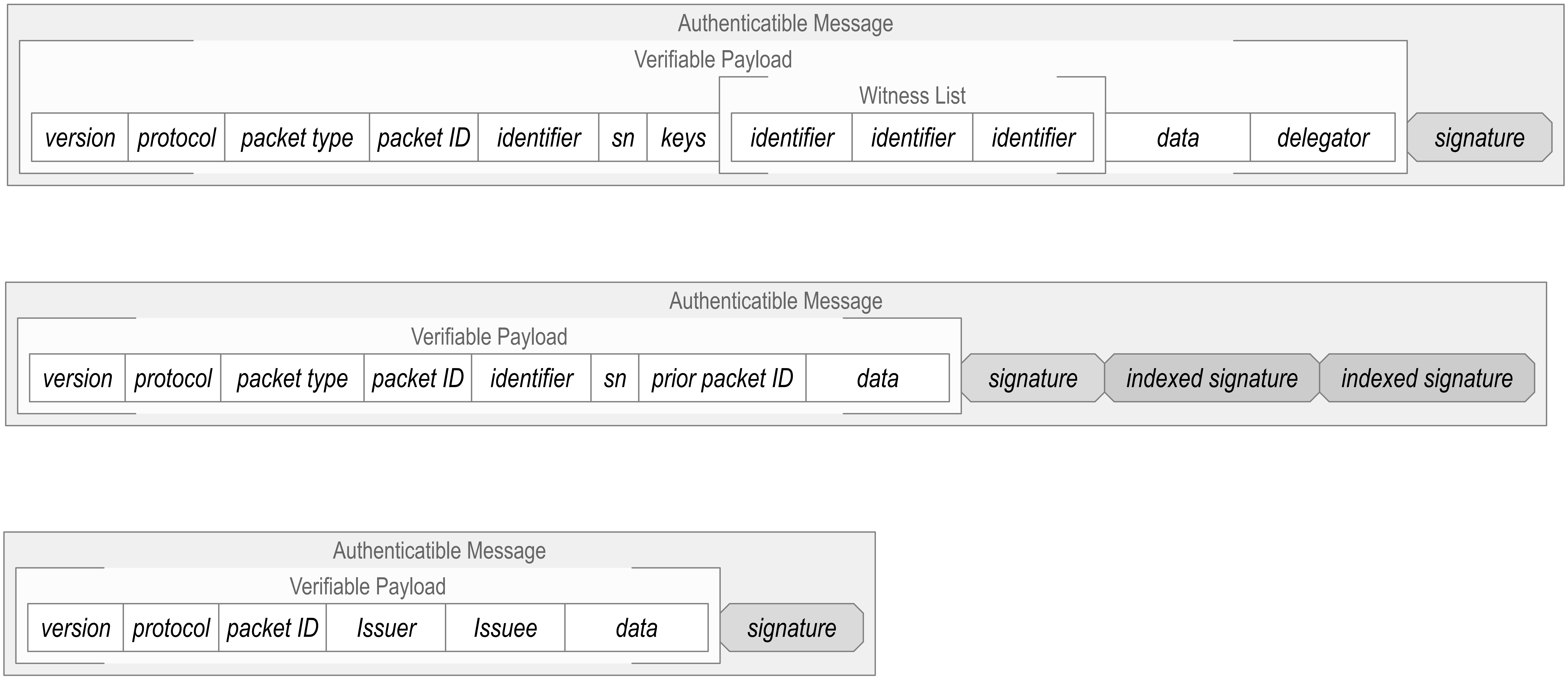
Key State Proof is Recursive Application of Overlay

persistent (transferable) mapping = verifiable data structure of key state changes



Wither *Destination* in Authentication Overlay

what counts as a *destination* identifier is contextual and may be entirely implicit



Confidentiality Overlay Duality

A confidentiality overlay is the *dual* of an authenticity overlay

- *Authenticity*: Asymmetric key pair for signing, private key signs, any public key verifies
  - Only the key pair controller can sign with the private key, any recipient can verify with the public key.
- *Confidentiality*: Asymmetric key pair for en-de-cryption, public key encrypts, private key decrypts
  - Only the key pair controller can decrypt with the private key, any sender can encrypt with the public key

Any identifier can have a key state that includes both an asymmetric signing key pair and an asymmetric decryption key pair.

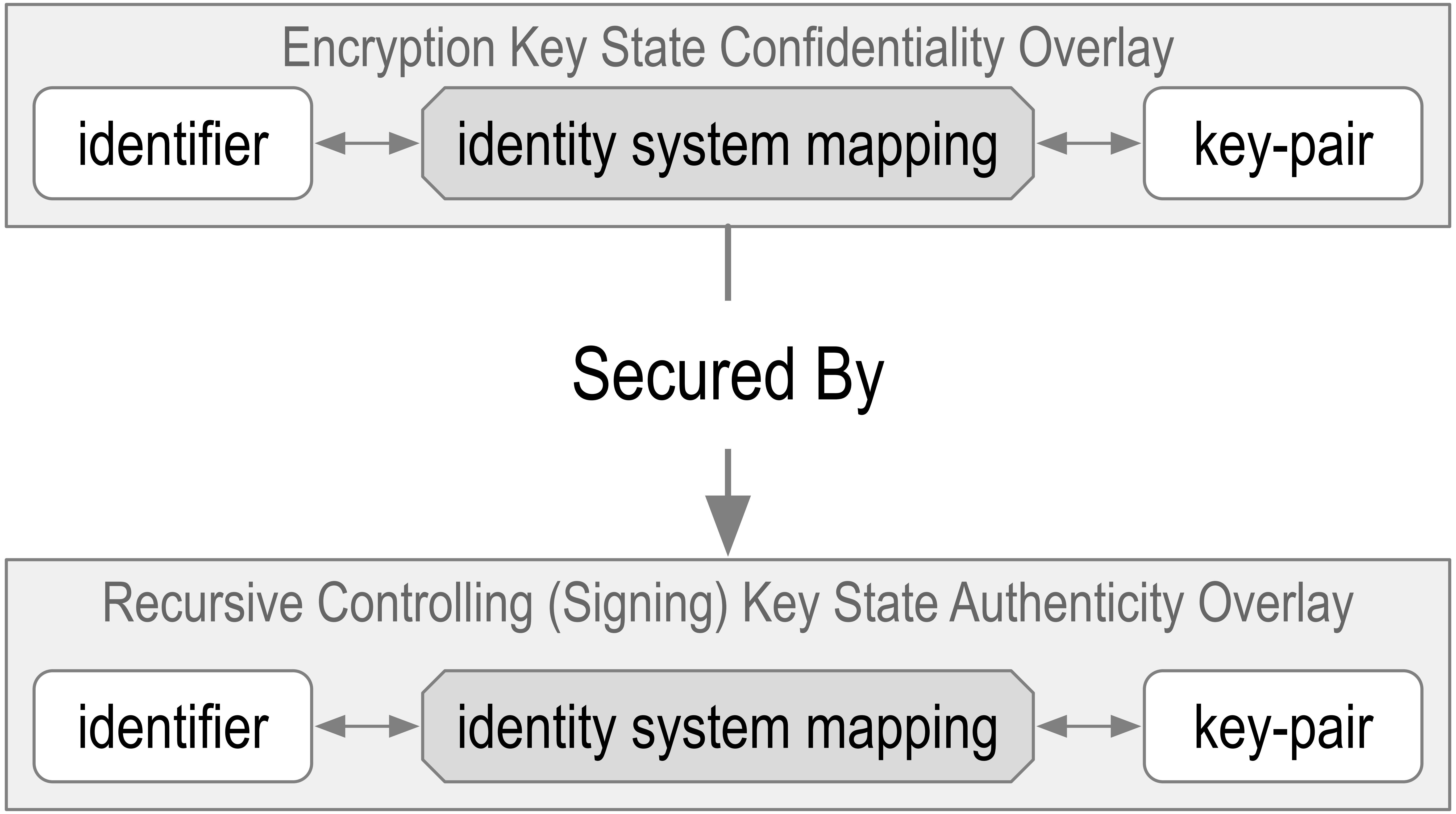
- Either the key pairs can be the same, or the decryption key pair can be derived from the signing key pair
- Thus an efficient approach is that only one key state, the signing key state, needs to be maintained. (with caveats)

Given the identifier and the security overlay's mapping to look up key state, any other party:

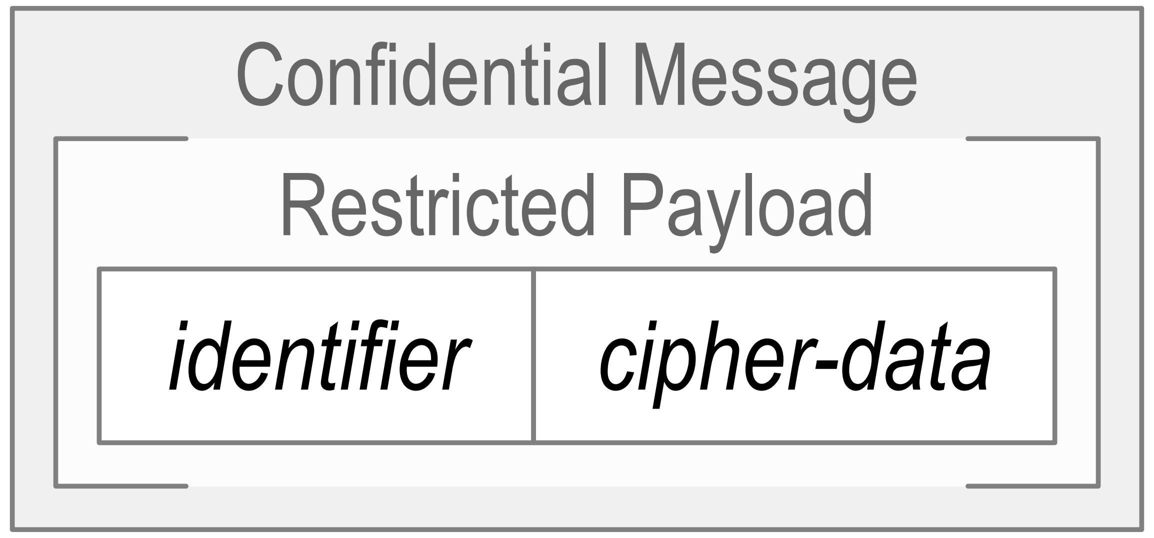
- Can verify with the signing public key that a message was non-repudiably sourced by the controller of the identifier (authenticity) (any-end-verifiable non-repudiable)
- Can encrypt a message using the encryption public key to ensure that only the controller of the identifier can view it (confidentiality) (only-end-viewable restricted)

Confidentiality Overlay Dependency

The encryption key state mapping can leverage the same persistent control mechanism as the signing key state mapping.
Indeed, the encryption key state must be securely attributable to the intended identifier for confidentiality to work.
In this strong sense, the confidentiality overlay depends on the authenticity overlay.



Confidentiality Overlay Elements

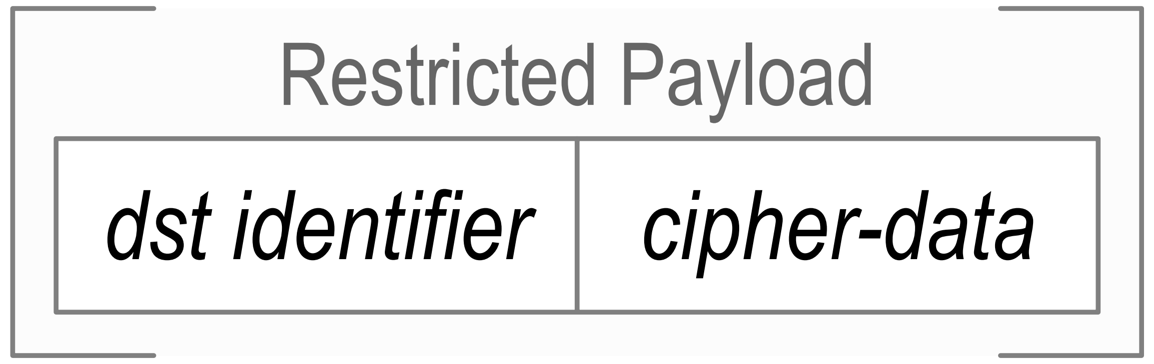


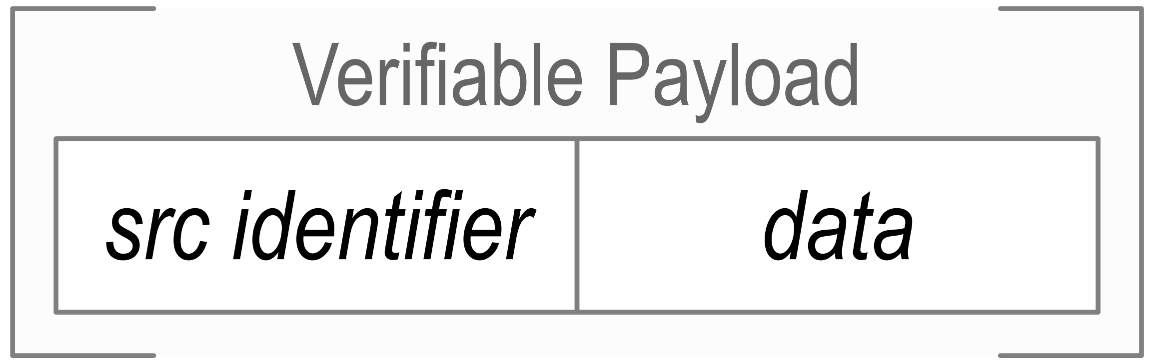
Strong Confidentiality Features:

3 party model: 1st party is sender, 2nd party is intended receiver, 3rd party unintended receiver

- 3rd party non-viewability
- 2nd party partition-ability by 1st party
  - Detectable leakage (2nd party to 3rd party)
  - Detectable collusion (2nd party to 2nd party)
- 1st party non-view-ability (protects 1st party from liability, protects 2nd party from exploit of 1st party via shared secret)
- 1st party non-collude-ability by 2nd party (1st party to 1st party or 1st party to 3rd party)

Layering Confidentiality & Authenticatability Overlays

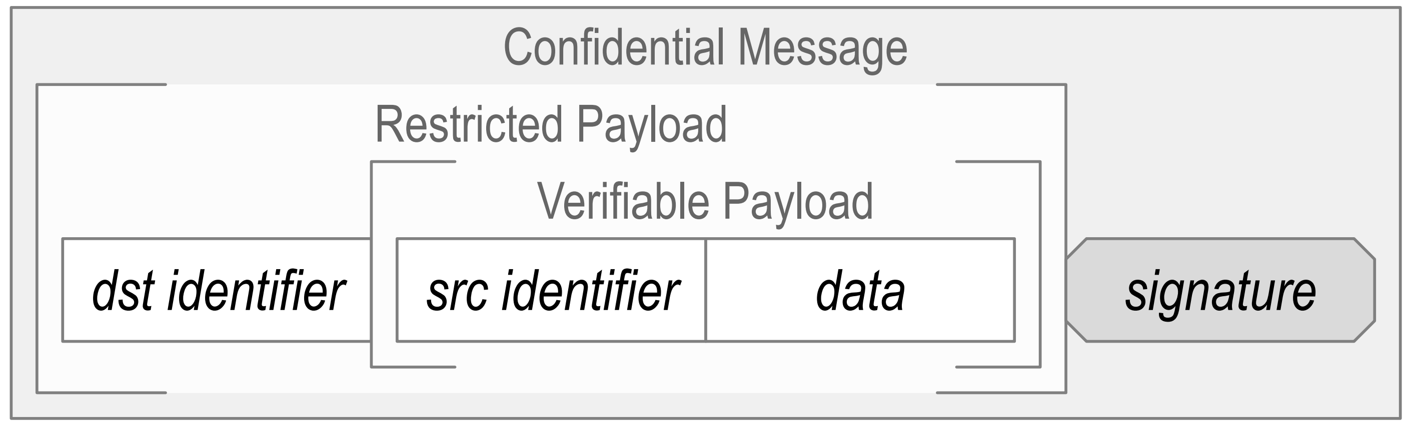


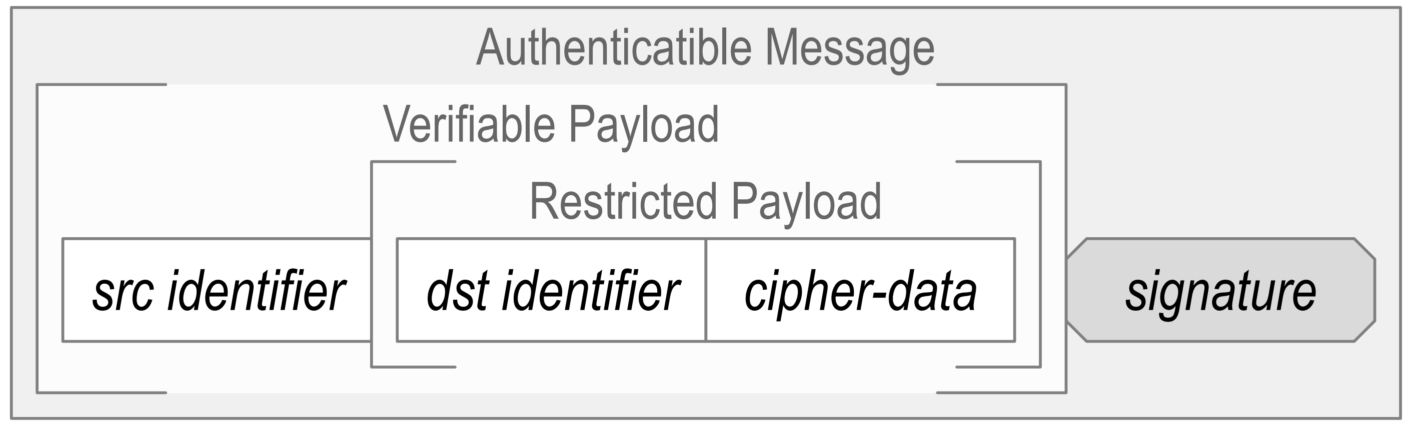


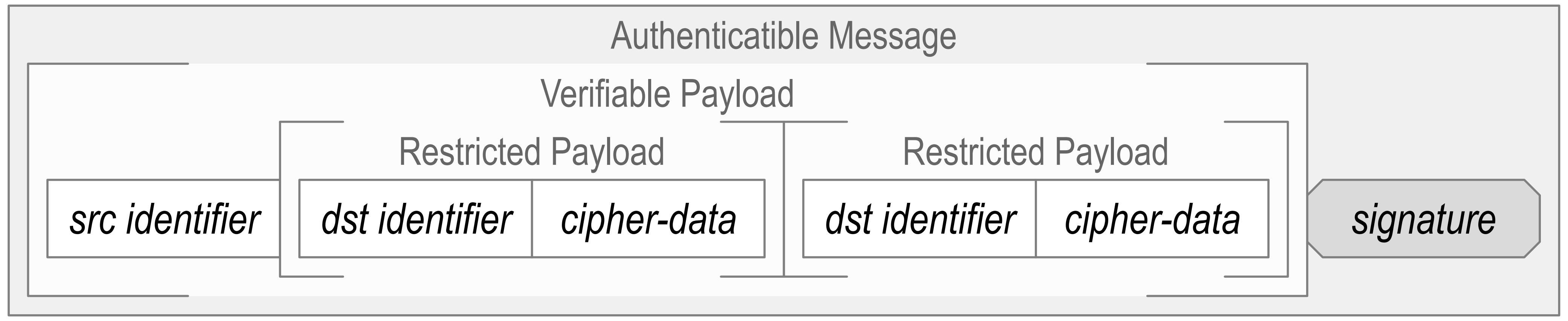
Setups matter! Order of layering is setup dependent, including the setups of any trusted intermediaries

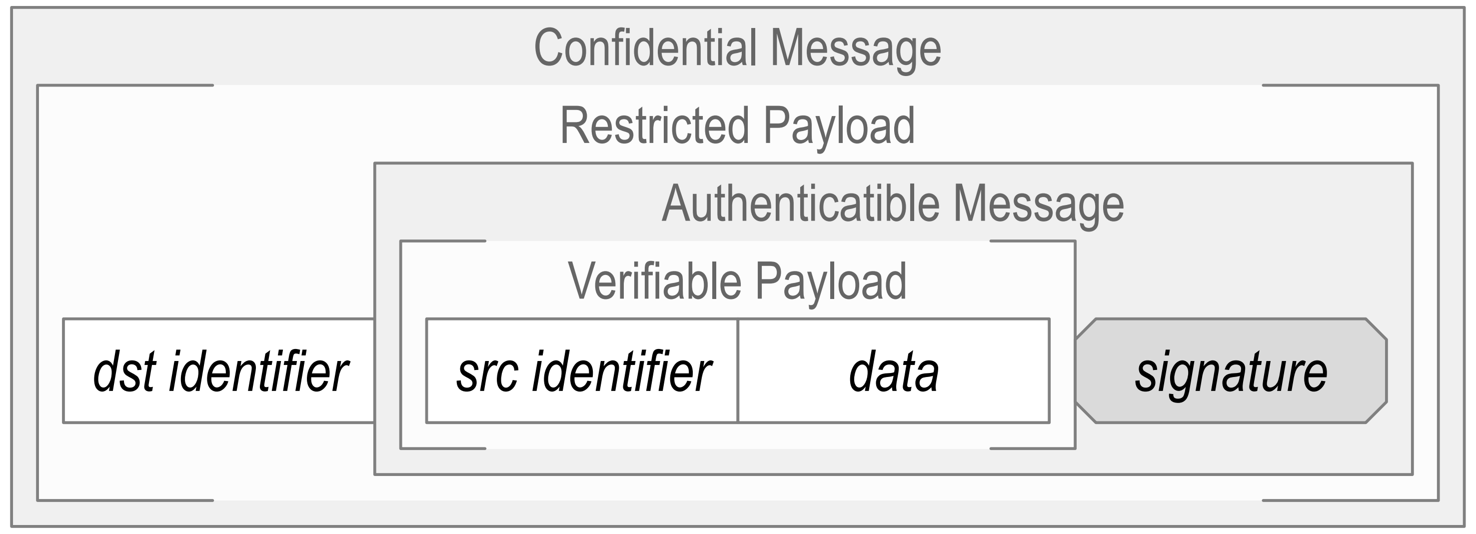
The presence or absence (explicit vs. implicit) of src and dst identifiers in a message is setup dependent

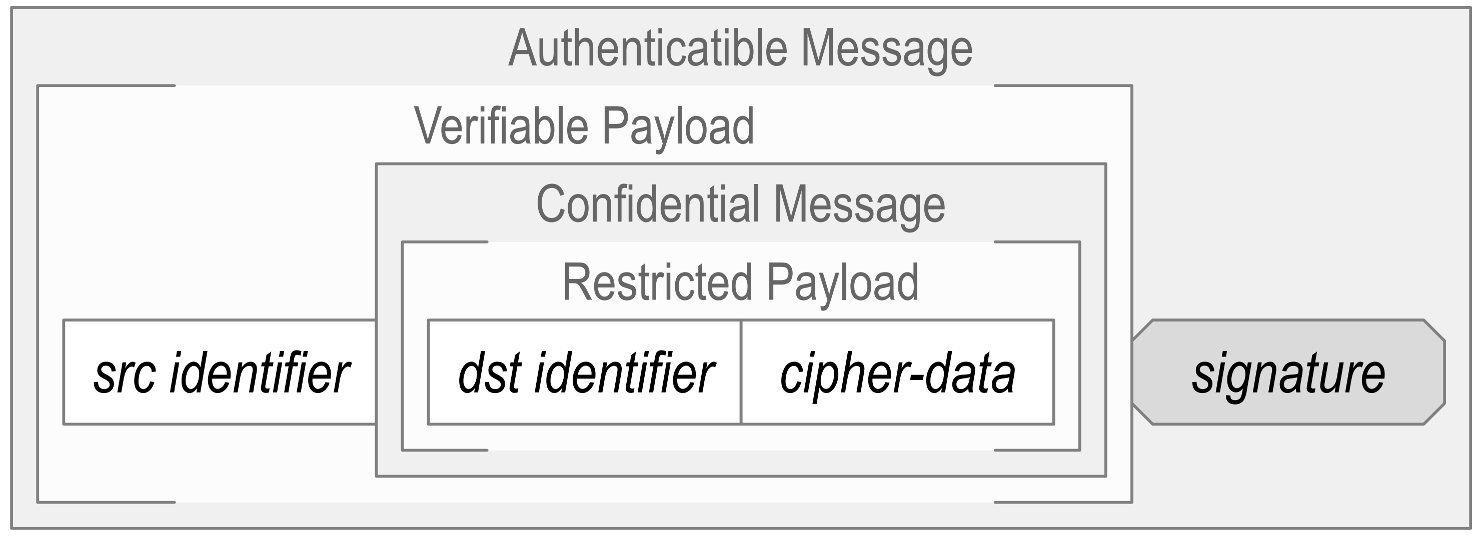
The hard problem of setups for persistent identifiers is to avoid repeating non-scalable manual setups like OOBA in order to ensure persistent control (solved by pre-rotated provenanced key state on cryptographic root-of-trust)











Overlay: Protocol Abstraction vs. Concrete Interaction

Overlay as a protocol abstraction where protocol determines type of overlay
hence types of trust basis, trust domain, roots-of-trust, and interactions, …
versus …
Overlay as a concrete application of a specific identifier's trust basis.
Concrete instantiation of any of the abstract types is per identifier not per identifier type!
Any interaction is concretized by a given message or set of messages wherein each message may involve multiple identifiers, each with a different controller and hence a different concrete trust basis.
The type of a given trust basis determines the type of its trust domain.
What happens when a given concrete interaction as overlaid message(s) mixes identifiers from trust bases of different types and hence trust domains of different types?
Is an ITDP even sensible in such a scenario?

Trust Domain Appraisability

Trusted computing group uses the term *appraisal* to refer to the process of evaluating roots-of-trust for their security properties with regards the security policy of what is acceptable data secured by that root-of-trust (see also IETF RATS).

Generalizing, an *appraisable* trust-basis of some party to an interaction can be evaluated by any other relying party to that interaction with respect to the relying party's data acceptance policy.

How difficult is the appraisal of a given trust basis?

Some types of trust bases may have well-known easily appraisable characteristics that better facilitate trust transitivity in any given interaction relying on that trust basis versus other types of trust bases.

Maximal trust transitivity happens in an interaction when the trust bases of all parties are mutually appraisable with the same degree of trustability and at relative low appraisal cost.

Types of Trust Bases

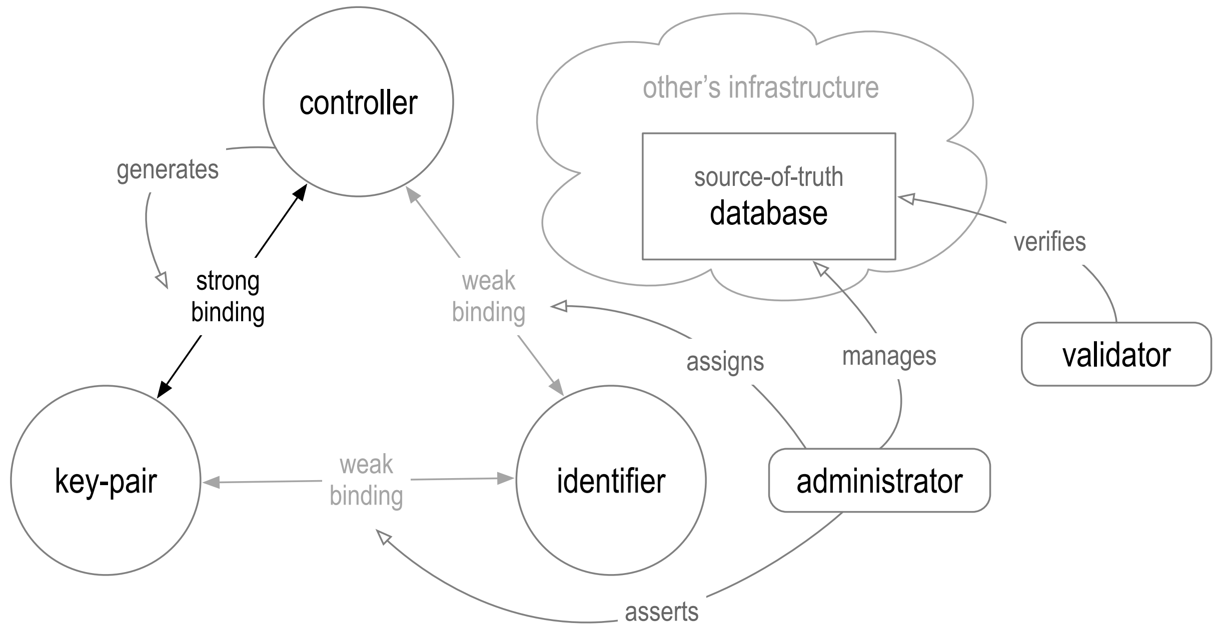
Given that maximal trust transitivity happens in an interaction when the trust bases of all parties are mutually appraisable with the same degree of trustability and at relative low appraisal cost …

Should we be fostering interoperability in interactions between poorly appraisable trust bases that either hide the security weaknesses or limit trustability to the lowest common denominator?

Analogy: Once non-repudiable digital signatures (using PKI) were invented, best practices deprecated HMACs for signing.

Is it not ludicrous to have a signed agreement where some parties use digital signatures, and some use HMACs?

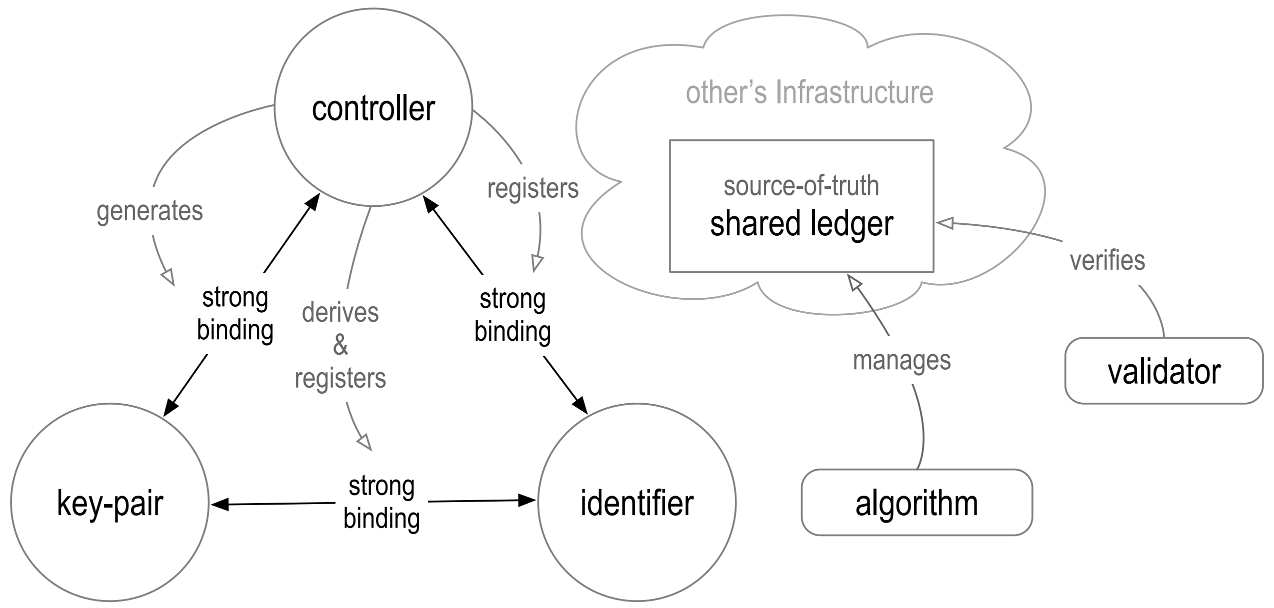
Administrative
DNS/CA



Opaque

Impractically High Appraisal Cost

Algorithmic
Shared Distributed Ledger



Duplicity Hiding

Non-monotonic (revisable)

Non-portable

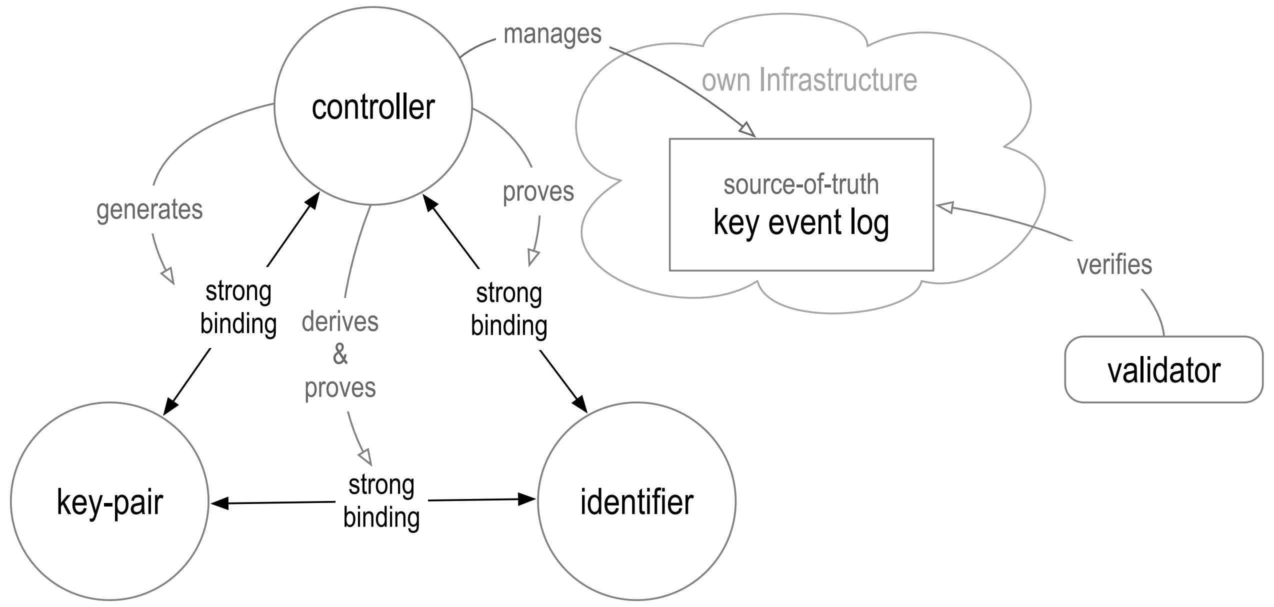
Shared Control

Algorithmic Strength

More or Less Zero Trust

Relatively high appraisal cost

Autonomic
Cryptographically Verifiable



Duplicity Evident

Monotonic (non-revisable)

Portable

Non-Shared Control

Cryptographic Strength

Fully Zero Trust

Relatively low appraisal cost

Zero-Trust Architecture: Data Protection

Never Trust, Always Verify

- Perimeter-less Security Model (necessary but not sufficient)
- Zero-Trust Spectrum = *ratio* of *trusted* surface to *verifiable* surface
- Trade-space axes of verifiable trust are *authenticity*, *confidentiality*, *privacy*
  - All protected data must have end-verifiable non-repudiable authenticity to its source (signing)
  - All protected data may have end-only viewable confidentiality to its destination (encrypting)
  - All protected data may have sufficient privacy amongst the parties to that data (correlating)

Data is signed and/or encrypted both *in motion* and *at rest* *(overlays should support both)*

- *at rest* means the storage mechanism is a *party* to the conversation
- *at rest* is an attack surface that *in motion* can't protect against
- party identifiers may be *explicit* or *implicit* w.r.t protected data

Intellectual Honesty vs Advocacy

Intellectually Honest Seekers of Truth and Tellers of Truth

Harvard ethicist Louis M. Guenin describes the "*kernel*" of intellectual honesty to be "*a virtuous disposition to eschew deception when given an incentive for deception.*"[1]

Being an ***intellectually honest*** *seeker and teller of the truth* means you make arguments you think are true, as opposed to making the arguments you are "*supposed*" to make and avoiding making arguments that you think are true that you aren't "*supposed*" to make.

"To tell the truth, rightly understood, is not just to state the true facts, but to convey a true impression." —Robert Louis Stevenson

Advocates, by contrast, make the best arguments they can think of for the *position* that they are *obliged* to take by their *position*. They are still supposed to be honest – they are not supposed to "*actually*" lie. But they are not expected to follow their own *consciences* regarding the arguments they make or the positions they advance.

Adversarial Advocates depend on an impartial arbiter (3rd party Judge, Jury, etc) to ensure "honesty". The advocates are largely absolved of dishonesty in their advocacy unless held accountable by the arbiter.

Intellectual Honesty

Intellectual honesty is honesty in the acquisition, analysis, and transmission of ideas.

A person is being intellectually honest when he or she, knowing the truth, states that truth.

The intellectually honest are not merely ***truth-seekers*** but have the courage to be ***truth-tellers*** even when it is not in their best interests.

So "*intellectual honesty*" is, in a sense, a higher standard than mere "*honesty*". And while *dishonesty* in argument is pretty much always a bad thing—you can imagine extreme "murderer at the door" counterexamples, of course—it's not clear that "*intellectual honesty*" is necessary in every context.

Sometimes—as in a debate round or an adversarial legal proceeding—you want everyone to make the strongest case they can for whatever position they're assigned to defend, regardless of their own view, to get a clear contrast—or "good clash," as we used to call it. Sometimes the point is working consensus rather than a search for some ideal.

In a world where people, including intellectuals, often pursue *incentives* more eagerly than they seek after *high ideals*, the more complicated the issue and the murkier the facts, the easier it may be for an intellectual to get away with presenting a plausible but flawed argument.

If *intellectual dishonesty* is to be consistently avoided, it is important that ways be found to make the interests of intellectuals coexist with the interests of those whose well-being depends on their intellectual honesty.

Intellectual Dishonesty

Some intellectual dishonesty can be subtle. For example, relevant facts and information may be purposefully omitted when such things contradict one's hypothesis, or facts may be presented in a biased manner or twisted to give *misleading impressions*.

Broadly speaking, any of the following behaviors would fall under intellectual dishonesty:

- Arguing for a viewpoint you yourself disbelieve.

    - *Exception*: The role of *devil's advocate*, when consciously acted out, is not intellectually dishonest. A good devil's advocate will express the opposition's strongest arguments and draw attention to the weaknesses of the arguments of co-thinkers. This is a valuable tool for intellectual rigor and honesty, and also helps to ward off the dangers of echo chambers and the resulting groupthink.

- Deliberately ignoring facts and arguments that would undermine your position. (willful ignorance)

- Knowingly using a logical fallacy such as equivocation, plagiarism, applying double standards, presenting straw man arguments, poisoning the well, using false analogies, exaggeration, or overgeneralization, etc.