

Update on the
Universal Name System (UNS) and **Universal Certificate Authority (UCA)**

Stop Leaky Computing

Universal Name System (UNS)

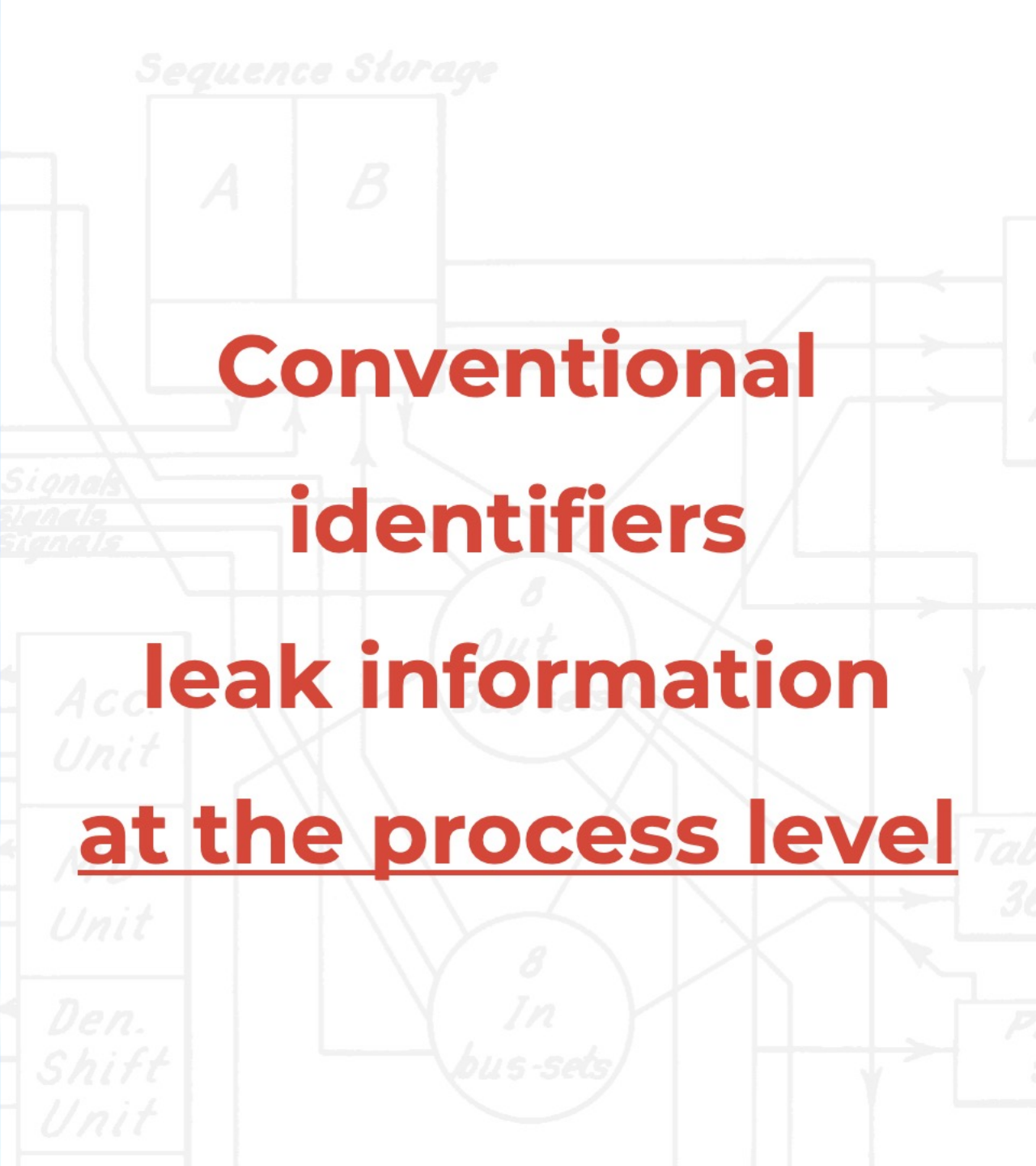
A global, decentralized, automated, zero-trust cryptographic name system unified across all types of entities: people, organizations, physical things, and digital things

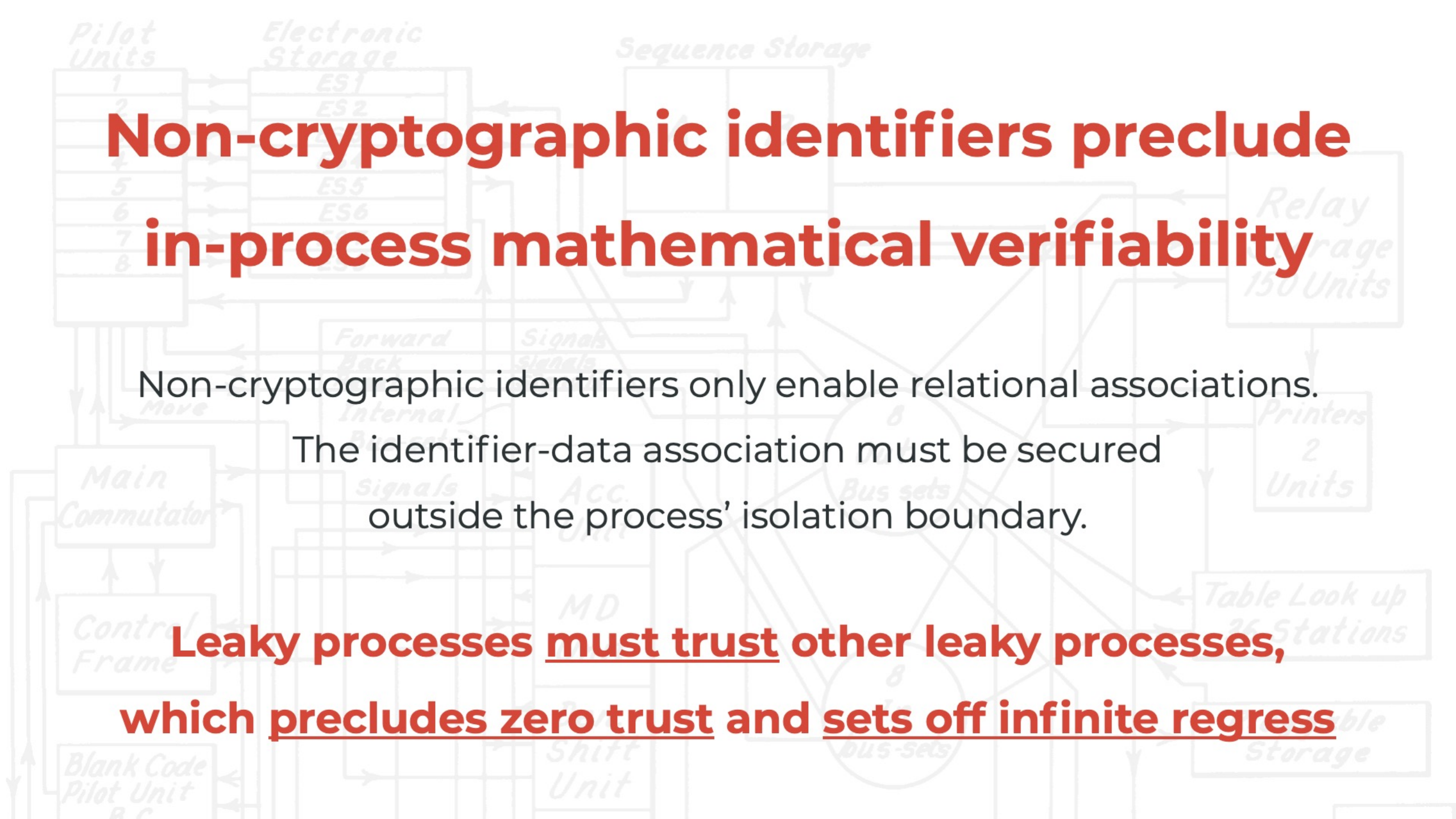
Universal Certificate Authority (UCA)

A global, decentralized, automated, zero-trust key infrastructure to solve provenance, integrity, authenticity, reputation, confidentiality, and privacy



**Conventional
identifiers
leak information
at the process level**



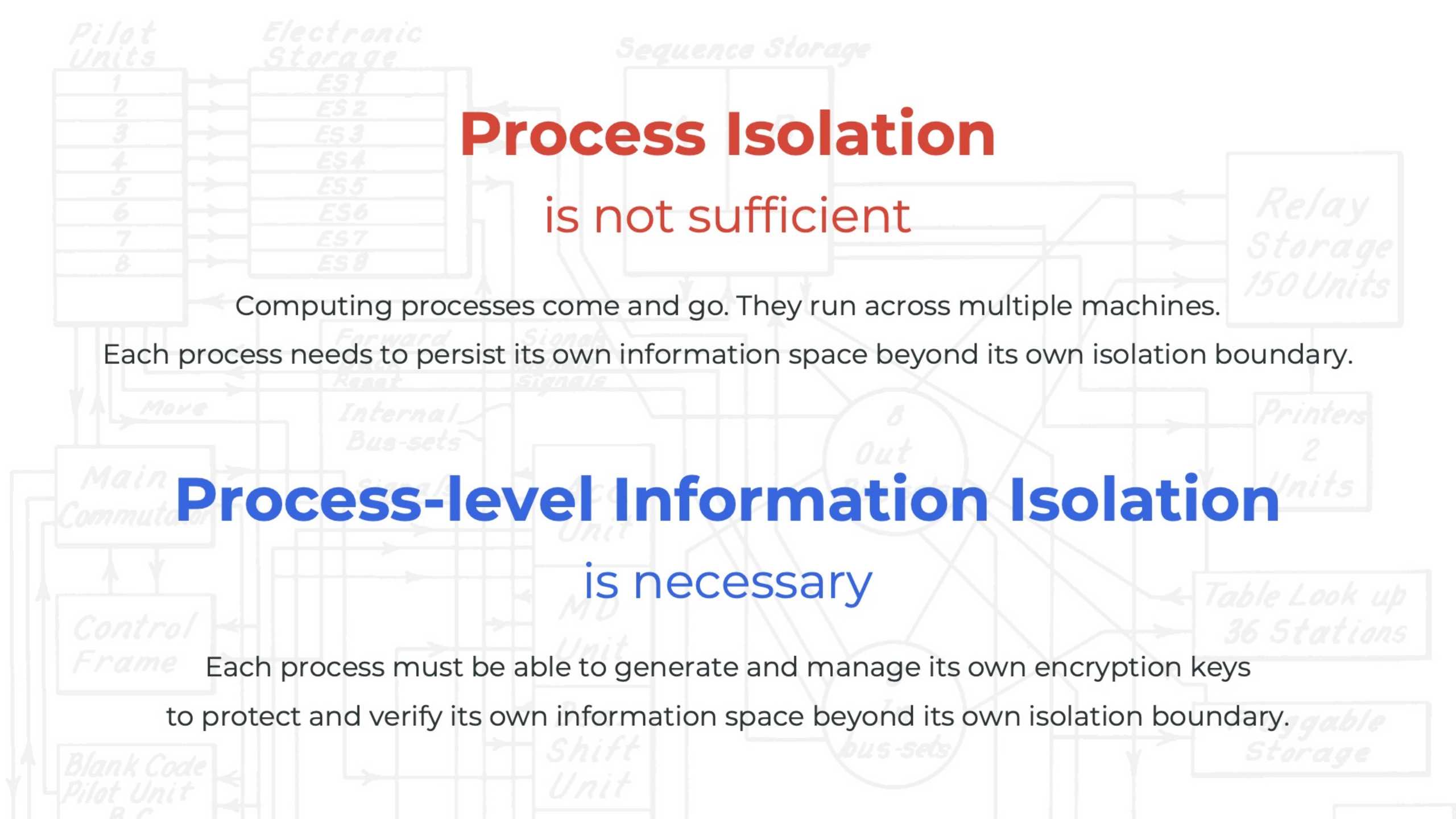


Non-cryptographic identifiers preclude in-process mathematical verifiability

Non-cryptographic identifiers only enable relational associations.

The identifier-data association must be secured outside the process' isolation boundary.

Leaky processes must trust other leaky processes, which precludes zero trust and sets off infinite regress



Process Isolation is not sufficient

Computing processes come and go. They run across multiple machines.
Each process needs to persist its own information space beyond its own isolation boundary.

Process-level Information Isolation is necessary

Each process must be able to generate and manage its own encryption keys
to protect and verify its own information space beyond its own isolation boundary.

Stem Identifier

(StemID)

Full-entropy random 256-bit identifier
(Exclusively generated and managed within TEEs)

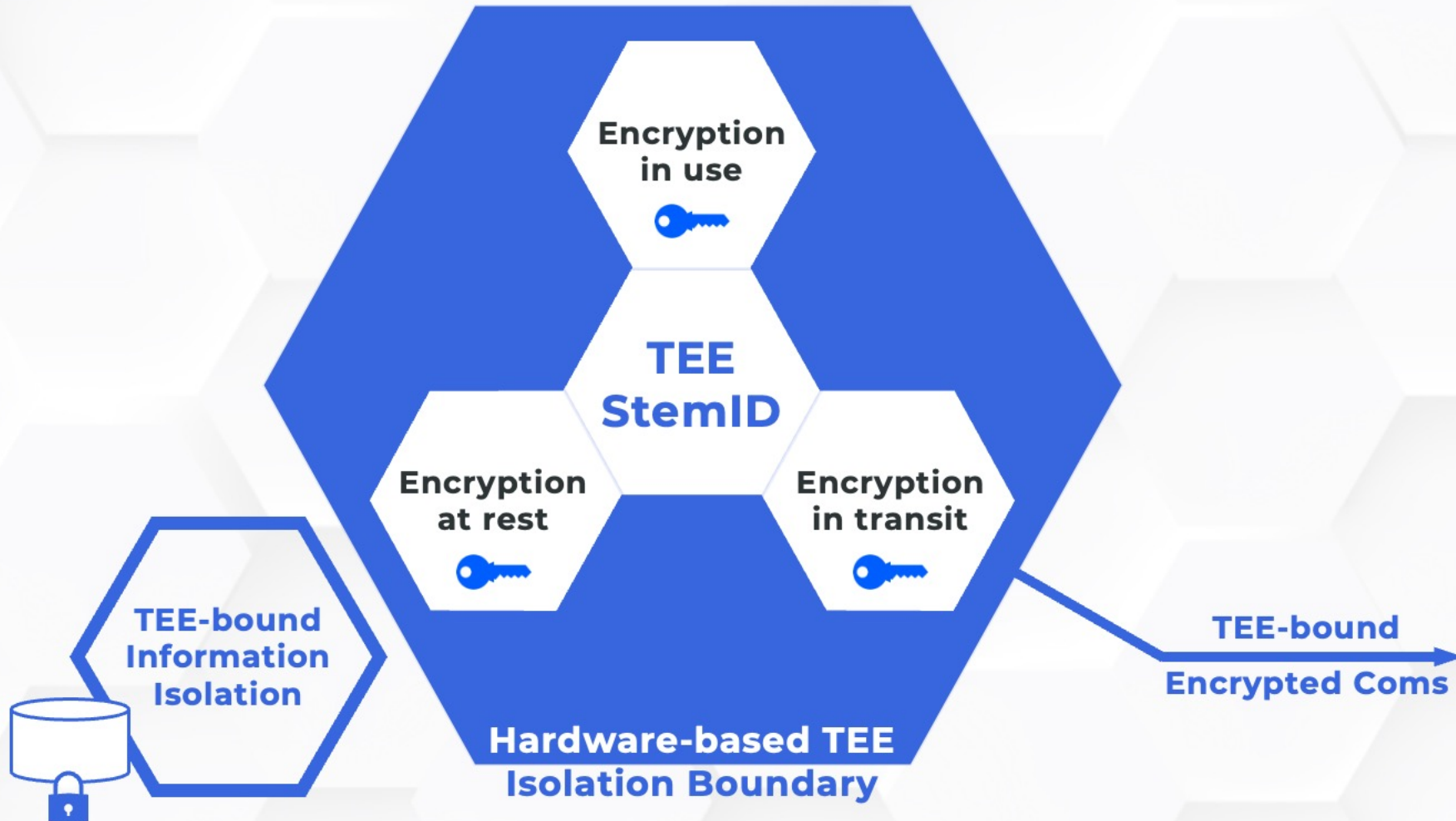
**Identifier AND symmetric key simultaneously
which enables key derivations from the identifier itself**

Example:

c1KXzxfVRf1JIJYVKq4zMGixUBGOF3J4LRrDHeJxpHk

StemIDs unify **seamless, universal, and zero-trust**

TEE-bound Authenticated Encryption



Why bring this work to the IETF?

**Not leaking information
makes the internet work better**

Side Meeting in **Meeting Room 2** on **Tuesday @ 17:00**

UNS / UCA overview, updates, and conversation

Discuss collaboration and coalition for neutral governance

Figure out **whether/how to bring this work to the IETF**

manu@hushmesh.com