

July 2026 Non-confidential Physical trust

The physical evidence gap

AI can generate convincing digital evidence. Critical systems still need a dependable basis for trusting what happened in the physical world.

DIGITAL CLAIM

identity · record · instruction

PHYSICAL REALITY

person · asset · action

CONTROLLED DECISION

permit · deny · escalate

4SI strengthens the point where digital trust meets the real world.

Why this matters now

Software transparency, cryptographic identity and hardware attestation are essential. Taken together, current work across IETF transparency standards and NIST hardware traceability also highlights a remaining boundary: a digitally valid record does not, by itself, establish that the claimed real-world person, asset or action was the one an organization intended to trust.

4SI is building physical trust infrastructure: a complementary control layer intended to connect high-consequence decisions to stronger evidence about real-world assets, authorized presence and operational provenance.

A control layer for high-consequence systems

4SI is not a replacement for PKI, hardware attestation, transparency services, inventory systems or access control. The opportunity is to strengthen the physical boundary those systems ultimately depend on.

Where the problem appears

- **Secure AI infrastructure** Trust around sensitive hardware, facilities and authorized operational actions.
- **Defense and space systems** Resilient assurance across distributed equipment, communications and field operations.
- **Critical infrastructure** Higher-confidence maintenance, access and component handling in essential systems.
- **Advanced manufacturing** Improved provenance and custody for high-value or safety-critical assets.

Start with one consequential decision

The right starting point is not a broad deployment. It is one operational decision where existing digital controls leave a material physical uncertainty.

Decision Which decision depends on physical certainty?

Consequence What happens if the claim is wrong?

Boundary What do existing controls fail to establish?

Evaluation What outcome would justify deeper work?

SELECTED PUBLIC CONTEXT

These sources establish the public context for this perspective; the interpretation and proposed category are 4SI's own.

- 1 IETF SCITT charter and stated non-goals
- 2 NIST Semiconductor Traceability & Provenance Workshop (2026)
- 3 NIST / Google / Microsoft - Trustworthy Ingestion of Secure Silicon
- 4 NIST Securing AI Data Center Architecture workshop (2026)

ABOUT 4SI

4SI develops physical trust infrastructure for high-consequence systems across AI, defense, space, critical infrastructure and advanced manufacturing.

DISCLOSURE This overview excludes proprietary architecture, protocols, implementation methods, security parameters and unpublished results. References provide context only; no affiliation or endorsement is implied.

Published by 4SI / by4si.com