SCITT WG

Unique Identification & Semantic Correlation

Presenter: Henk Birkholz

<scitt@ietf.org>

IETF 127 San Francisco, 18th November



Identifiable but No Real Identification

- RFC 9943: a Signed Statement is “an identifiable and non-repudiable Statement about an Artifact signed by an Issuer”
- There is no actual statement identifier. What exists today:
  - **Subject (sub), Issuer (iss):** groups statements, no guarantee to select one
  - **Entry locator (SCRAPI):** local to one Transparency Service (TS)
  - **Position in the log:** never named as an identifier, not necessarily usable as an identifier
- Shepherd writeup: identification and references “may be addressed in a separate, later document”



Twice In, Twice Out

Date	What happened to identification and references
2022-03	Feed per Issuer, TS enforces sequence numbers
2023-10	Feed becomes sub, -04 adds typed references
2024-02	-05 drops typed references and sequence numbers, adds hash URNs
2024-11	IETF 121: locators chosen by the TS, no standard format
2025-02	Hash URNs removed
2025-09	Shepherd writeup: no consensus, later document
2026-09	Proposal to recharter for relation semantics



Semantic Correlation: Labels That Already Exist

Label	Included in Exemplary Specification
revises	SWID and CoSWID tag version, CycloneDX, CSAF, OpenVEX
supersedes, replaces	CoRIM, RFC Obsoletes, FAA ADs, CSAF 2.1, TCG RIM
corrects, amends	RFC errata, EU corrigenda, SPDX AMENDS, ISO
supplements	CoRIM, SWID, TCG Supplemental RIM
withdraws, retracts	CSAF, OSV, GS1 EPCIS, Crossref
revokes, suspends	X.509 CRL, W3C status list, OAuth status list
reaffirms	CISA VEX, ISO, NERC



Same Terms, Different Semantics in Existing Work

- **Link direction:** old points to new (CSAF, CVE), new points to old (CoRIM, TCG RIM), no link (X.509, RFC 9943)
- **The old statement:** “MUST be disregarded” (CoRIM) or stays valid (ACME ARI, EU harmonized standards)
- **Reversible:** CVE rejection yes, W3C revocation no
- **“supersedes”:** software (SWID), revocation reason (X.509), statements (FAA, CSAF)
- **“ancestor”:** previous release (CoSWID), fork origin (CycloneDX)



Proposal for Discussion

- **Reference:** e.g., a digest of the opaque payload, not only iss & sub
- **Relationship Types:** small number of relations, content-type agnostic
- **Consumer rules:** per label, the intended purpose of the referred-to statement, and if that purpose can change
- **Order:** explicit relations, not inferred from log order
- **Ask:** recharter SCITT for relation semantics between statements?
- **Question:** Where do relation semantics go? (e.g., into the Signed Statement protected header, into a non-opaque standard payload wrapper, etc.)



Sources

- RFC 9942, RFC 9943, draft-ietf-scitt-scrapi-11, draft-ietf-scitt-receipts-ccf-profile-06
- draft-gruszka-scitt-statement-identification-03
- scitt list: shepherd writeup (2025-09-10), relation semantics (2026-09-21), statement ID requirements (2026-09-22)
- NIST IR 8060, RFC 9393, CoRIM, SPDX 2.3 and 3.x, CycloneDX 1.7, CSAF 2.0 and 2.1, OSV, CVE, RFC 5280, W3C Bitstring Status List, GS1 EPCIS 2.0, FAA ADs, EU law (ELI)

