

Integrity Protection of IOAM Data Fields

[draft-ietf-ippm-ioam-data-integrity-13](#)

Justin Iurman, Frank Brockners, Shwetha Bhandari, Tal Mizrahi

IETF 122, IPPM WG
March 18, 2025

Status -13

- Back from WGLC to WG Document
- -14 is work in progress: address secdir's review (+ review from Giuseppe Fioccola)
- 2 main issues:
 - ◆ reuse of Nonce on transit nodes (needs more text from a security point of view)
 - easy to address, proposed text by the reviewer
 - ◆ header fields included in the integrity protection vs. interoperability
 - persisting issue between versions, multiple (trade-off) solutions

Solution for header fields and interop?

Current solution: define header fields to be included, new ones are excluded (one-time fixed definition)

Opposite solution: versioning (perfect? maybe, but probably extreme)

- IOAM Option-Types (RFC 9197) don't have versions
- Would be (even) less hardware friendly...

Proposed trade-off solution: define header fields to be included, new ones are added to the registry

- Integrity protection seen as a feature on top of IOAM Option-Types
- This *feature* (if present) is aligned and up-to-date with its IOAM implementation
- If Vendor_A_IOAM **!=** Vendor_B_IOAM → no interoperability
- If Vendor_A_IOAM **==** Vendor_B_IOAM → interoperability (both IOAM and IOAM Integrity)