

Integrity of In-situ OAM Data Fields

[draft-ietf-ippm-ioam-data-integrity-03](#)

Frank Brockners, Shwetha Bhandari, Tal Mizrahi, Justin Iurman

IETF 116, IPPM WG
March 27, 2023

Status

- -03 published after IETF 115 (London)
 - IANA (early allocation approved)
 - editorial changes
- Pending modifications for -04:
 - Fix the integrity validation algorithm
- ACK from the implementor

Reminder

Rule: *an IOAM node only signs data fields it writes*

... data fields modified by other IOAM nodes are excluded from the signature

Reminder

Rule: *an IOAM node only signs data fields it writes*

... data fields modified by other IOAM nodes are excluded from the signature

E2E Option-Type:

- encapsulating node signs its data fields
- no transit node involved
- decapsulating node checks the signature of the encapsulating node

POT (Type 0) Option-Type:

- encapsulating node signs its data fields (**“Cumulative” field is excluded**)
- transit nodes only modify the “Cumulative” field
- decapsulating node checks the signature of the encapsulating node

Reminder

Rule: *an IOAM node only signs data fields it writes*

... data fields modified by other IOAM nodes are excluded from the signature

Trace Option-Type:

- encapsulating node signs its data fields
- each transit node signs its data fields
- decapsulating node checks the signature chain (from last transit node to encapsulating node)

Header protection?

Rule: *an IOAM node only signs ~~data fields~~ what it writes*

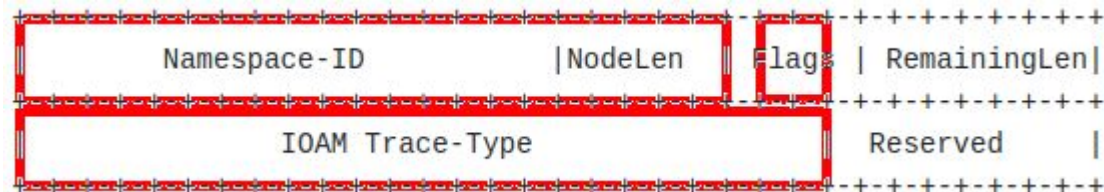
... ~~data~~ fields modified by other IOAM nodes are excluded from the signature

Header protection?

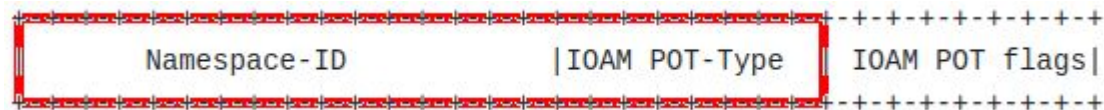
Rule: an IOAM node only signs ~~data fields~~ *what* it writes

... ~~data~~ fields modified by other IOAM nodes are excluded from the signature

- Trace Option-Type Header:



- POT Option-Type Header:



- E2E Option-Type Header:



Next

- Header protection?
 - Put back DEX Option-Type support