Integrity of In-situ OAM Data Fields

draft-ietf-ippm-ioam-data-integrity-06

Frank Brockners, Shwetha Bhandari, Tal Mizrahi, Justin Iurman

IETF 117, IPPM WG
July 24, 2023

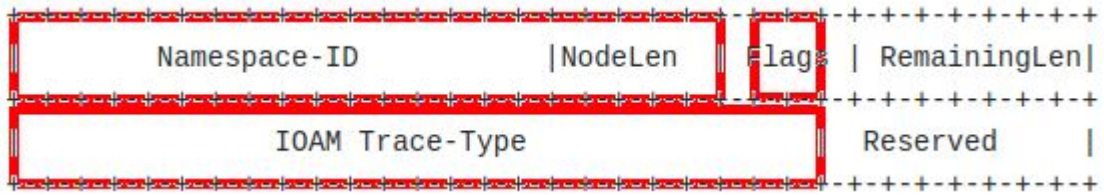
Status -06

- Added IOAM Option-Types header protection
  - allows to add DEX
  - updates the Validator role
- Removed the asymmetric key based signature algorithm
- Improved the security section
- Editorial changes

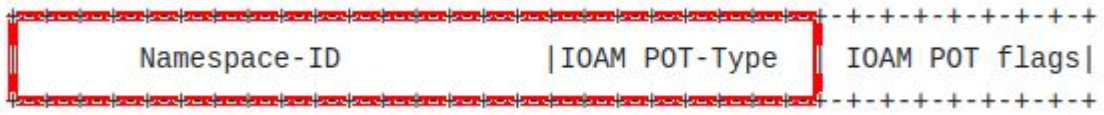
Header protection

Rule: *an IOAM node only signs ~~data fields~~ what it writes (i.e., adds) … ~~data~~ fields modified by other IOAM nodes are excluded from the signature*

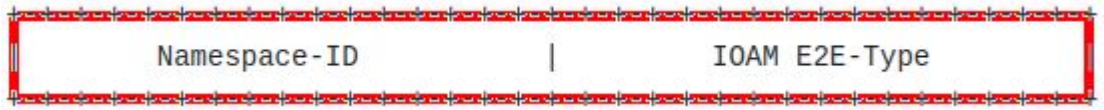
- Trace Option-Type Header:



- POT Option-Type Header:

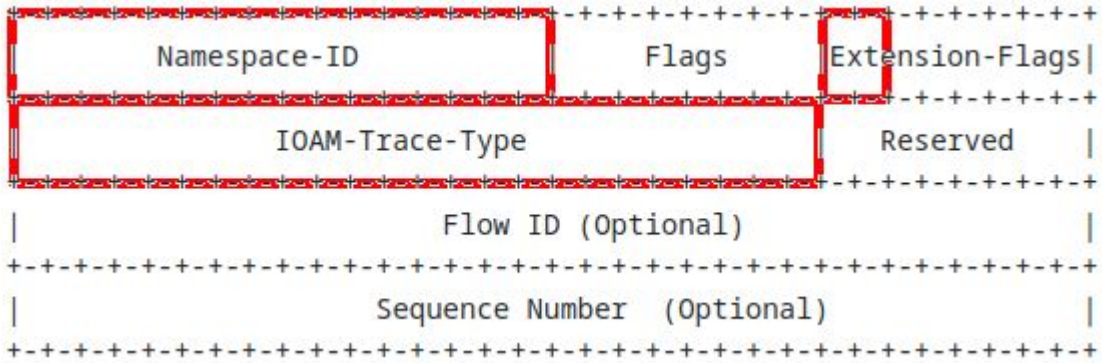


- E2E Option-Type Header:



Header protection

- DEX Option-Type Header:



“*The optional fields (i.e., Flow ID and Sequence Number) are treated as optional IOAM-Data-Fields, not header fields.*”

“*A document defining a new IOAM Integrity Protected Option-Type MUST define the IOAM Option-Type header fields involved in the integrity protection of IOAM-Data-Fields.*”

Integrity protection

Rule: *an IOAM node only signs what it writes (i.e., adds)*

… fields modified by other IOAM nodes are excluded from the signature

E2E Option-Type:

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

POT (Type 0) Option-Type:

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

Integrity protection

"*Each node that takes actions triggered by fields in the IOAM Integrity Protected Option-Type header MUST act as a Validator. Otherwise, an attacker could modify the IOAM header along the path and change the actions a node performs.*"

- Integrity Protected Trace Option-Type (**if Loopback or Active mode is enabled**)
- Integrity Protected DEX Option-Type

Integrity protection

Rule: *an IOAM node only signs what it writes (i.e., adds)*

… fields modified by other IOAM nodes are excluded from the signature

DEX Option-Type:

- encapsulating node signs header fields (and its “data fields”, if any)
- **each transit node checks the signature of the encapsulating node**
- decapsulating node checks the signature of the encapsulating node

Trace Option-Type:

- encapsulating node signs header fields and its data fields
- **If Loopback or Active mode, each transit node checks the signature of the whole chain up to itself**. Each transit node signs its data fields
- decapsulating node checks the signature chain

Next

- Secdir review? WGLC?
- RFC9326bis to update RFC9326’s security section?