In-situ OAM Deployment
In-situ OAM Flags
In-situ OAM Direct Exporting
Integrity of In-situ OAM Data Fields

draft-brockners-opsawg-ioam-deployment-03

draft-ietf-ippm-ioam-flags-05

draft-ietf-ippm-ioam-direct-export-05

draft-brockners-ippm-ioam-data-integrity-02

IETF 111, IPPM
July 2021

In-situ OAM Deployment

draft-brockners-opsawg-ioam-deployment-03

Frank Brockners, Shwetha Bhandari, Daniel Bernier, Tal Mizrahi

IETF 111, IPPM
July 2021

Status and Next Steps

- Scope
  - Document IOAM deployment, tying all the different IOAM related specifications together.
  - Document focuses on IOAM deployment. draft-ietf-ippm-ioam-data-14 references the draft.
- Version 03 main changes:
  - Security considerations:
  - added discussion about mitigating eavesdropping, DoS/DDoS, and time synchronization attacks; reflecting SEC-DIR comments from IESG review of draft-ietf-ippm-ioam-data.
- Discussion
  - Document started in OPSAWG, though with IPPM covering all IOAM-related work, IPPM is the natural place to progress the work.
  - draft-ietf-ippm-ioam-data includes an informational reference, following last call comments and request from Ben Kaduk (Security AD) and Shawn Emery (Security Area Directorate).
- The authors believe the draft is ready for WG adoption.

In-situ OAM Flags
In-situ OAM Direct Exporting

draft-ietf-ippm-ioam-flags-05

draft-ietf-ippm-ioam-direct-export-05

IETF 111, IPPM
July 2021

Flags / Direct Exporting Drafts – Security

- There was an extensive security related discussion about these two drafts in IETF 110.
  - Comments from Martin Duke, Mirja Kühlewind.

- The authors believe the current versions of these drafts address the issues.
- Security-related updates in both drafts:
  - [DEX / Flags] Selective DEX / Loopback / Active at IOAM encapsulating nodes.
  - [DEX / Flags] Rate limiting of exported / looped back packets at IOAM transit nodes.
  - [DEX] Avoid pushing the DEX option onto exported packets.
  - [Flags] Avoid pushing IOAM with Loopback flag onto IOAM-encapsulated packets.
  - [DEX] Export to trusted nodes.

In-situ OAM Flags

draft-ietf-ippm-ioam-flags-05

Tal Mizrahi, Frank Brockners, Shwetha Bhandari, Ramesh Sivakolundu,
Carlos Pignataro, Aviv Kfir, Barak Gafni, Mickey Spiegel, Jennifer Lemon

IETF 111, IPPM
July 2021

Status and Next Steps

- Version 05 addresses the security-related comments from Martin.
  - As discussed on previous slides.

- Next steps:
  - The authors believe the draft is ready for WG last call.

In-situ OAM Direct Exporting

draft-ietf-ippm-ioam-direct-export-05

Haoyu Song, Barak Gafni, Tianran Zhou, Zhenbin Li,
Frank Brockners, Shwetha Bhandari, Ramesh Sivakolundu, Tal Mizrahi

IETF 111, IPPM
July 2021

Open Issues - Suggested Resolution

- Two open issues have been widely discussed on the mailing list and in previous IETF meetings.

- Issue 1: Hop Count field.
  Question: should the DEX option include an explicit Hop Count field, or is the Hop_Lim/Node_ID data field sufficient?
- WG chairs' suggestion:
  No explicit Hop Count field.

- Issue 2: DEX option length.
  Question: should the DEX option have a constant length, or should flags be used to indicate optional fields?
- WG chairs' suggestion:
  Flags to be used to indicate optional fields.

Status and Next Steps

- Changes in version 05:
  - Significant changes to address security issues raised by Martin, Mirja.

- Next steps:
  - Update the draft to reflect the resolution to the two open issues above.

Integrity of In-situ OAM Data Fields

draft-brockners-ippm-ioam-data-integrity-02

Frank Brockners, Shwetha Bhandari, Tal Mizrahi

IETF 111, IPPM
July 2021

Changes in -02

- Recommended method for integrity for IOAM options
  - Space optimized symmetric key based signing of options
  - Space optimized asymmetric key based signing of options
- Alternate methods documented in Appendix
- New integrity protected IOAM options
- Common sub-header in IOAM options for integrity protection
- Overhead considerations updated to use integrity protection on subset of the packets

IOAM Integrity Protected Options

- Each IOAM Option is extended to include Integrity Protected (IP) options by allocating the following IOAM Option-Types in the IOAM Option-Type registry

Option Type	Integrity Protection Option	Corresponding IOAM Option
64	IOAM Pre-allocated Trace Integrity Protected Option-Type	IOAM Pre-allocated Trace Option-Type
65	IOAM Incremental Trace Integrity Protected Option-Type	IOAM Incremental Trace Option-Type
66	IOAM POT Integrity Protected Option-Type	IOAM POT Option-Type
67	IOAM E2E Integrity Protected Option-Type	IOAM E2E Option-Type

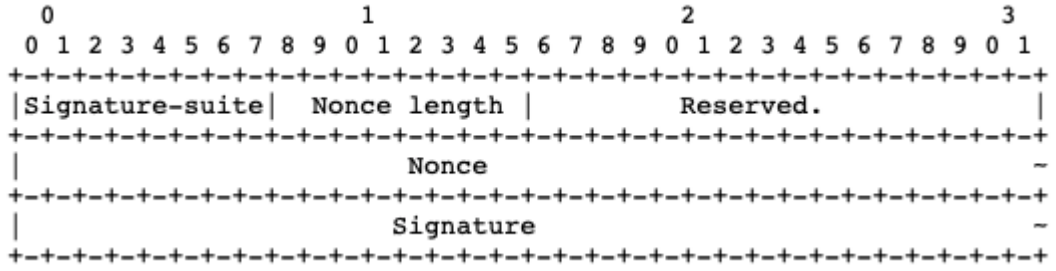
Integrity Protection sub-header format

Signature-suite: This field defines the algorithms used to compute digest and signature over the Option header and data excluding the Signature field
(e.g. Asymmetric key based method:
Suite: 0x1 :: Hash: SHA-256; Sign: ECDSA P-256
Symmetric key based method:
Suite: 0x2 :: Hash: SHA-256; Sign: AES-256)

Nonce length: This field specifies the length of the Nonce field in octets.

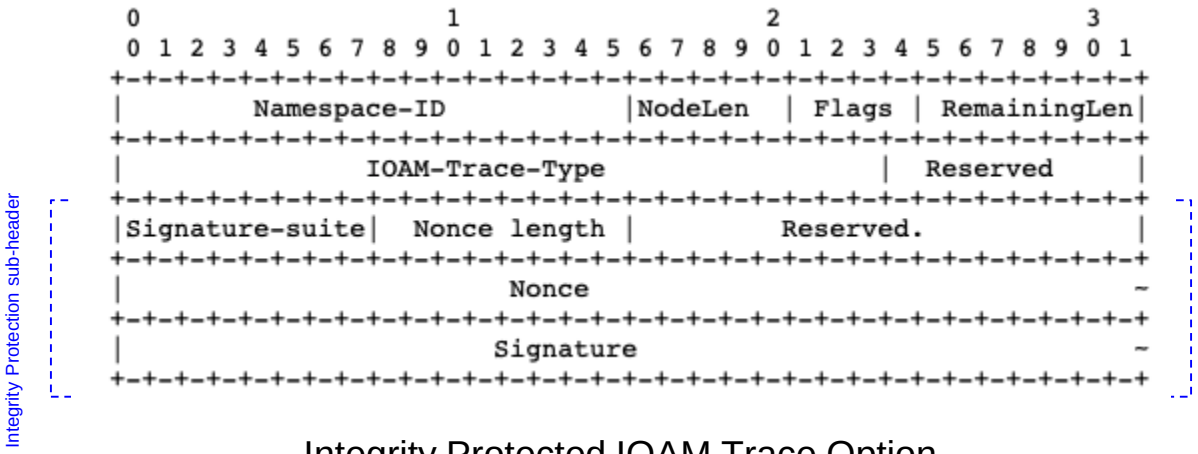
Nonce: Variable length field with length specified in Nonce length.

Signature: is the digital signature value generated by the method and algorithm specified by Signature-suite.

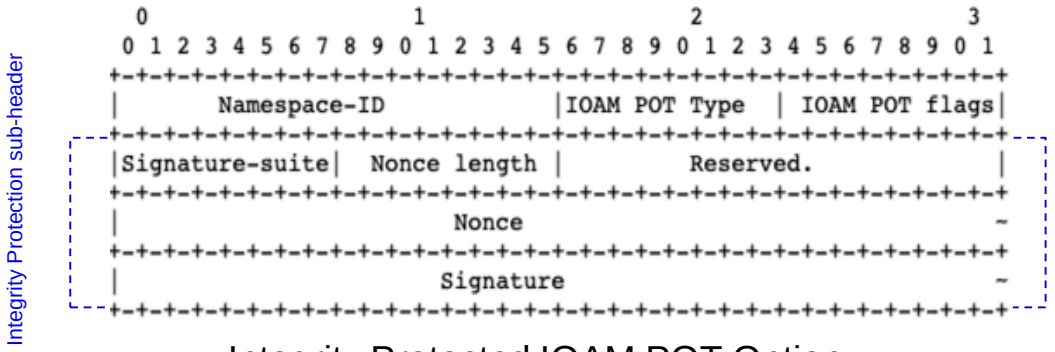


Integrity Protected IOAM Option

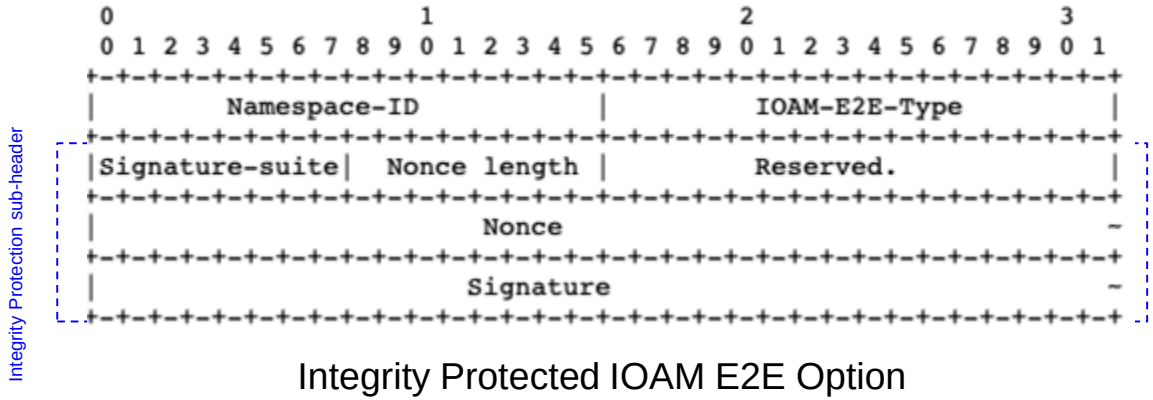
The Integrity sub-header will follow the IOAM Option header when the IOAM Option Type is Integrity Protected Option.



Integrity Protected IOAM Trace Option



Integrity Protected IOAM POT Option



Integrity Protected IOAM E2E Option

Status and Next Steps

- The feedback received in IETF 110 IPPM workgroup meeting and over mailer are discussed and addressed; draft-ietf-ippm-ioam-data-14 references the draft

- The authors believe the draft is ready for WG adoption.