

NV03  
Internet-Draft  
Intended status: Standards Track  
Expires: December 29, 2017

D. Migault  
June 27, 2017

Geneve Header Encryption Option (GEO)  
draft-mglt-nvo3-geneve-encryption-option-00

## Abstract

This document describes the Geneve Encryption Option (GEO). This option enables a Geneve forwarding element to encrypt the Geneve Header with selected associated Geneve Options as well as a portion of the Geneve Payload.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 29, 2017.

## Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Requirements notation . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">3.</a>	GEO Description . . . . .	<a href="#">2</a>
<a href="#">4.</a>	GEO Processing . . . . .	<a href="#">3</a>
<a href="#">4.1.</a>	GEO Placement . . . . .	<a href="#">3</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">7.</a>	Acknowledgment . . . . .	<a href="#">4</a>
<a href="#">8.</a>	References . . . . .	<a href="#">4</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">4</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">5</a>
	Author's Address . . . . .	<a href="#">6</a>

[1.](#) Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[2.](#) Introduction[3.](#) GEO Description

For generic format of the Geneve Options is defined in Figure 1. The following values are expected:

- o Option Class: 0x0000
- o Type: C is unset as the GEO can simply be ignored by a NVE or a transit node. The GSP will prevent to accept a GOA that is mandated by the GSP and that has not been validated.
- o R is set to 0.
- o Length: This document only considers the algorithms recommended by [[I-D.ietf-ipsecme-rfc7321bis](#)] ENCR\_AES\_GCM\_16 or ENCR\_CHACHA20\_POLY1305. These algorithms are defined in [[RFC4106](#)] and [[RFC7539](#)].

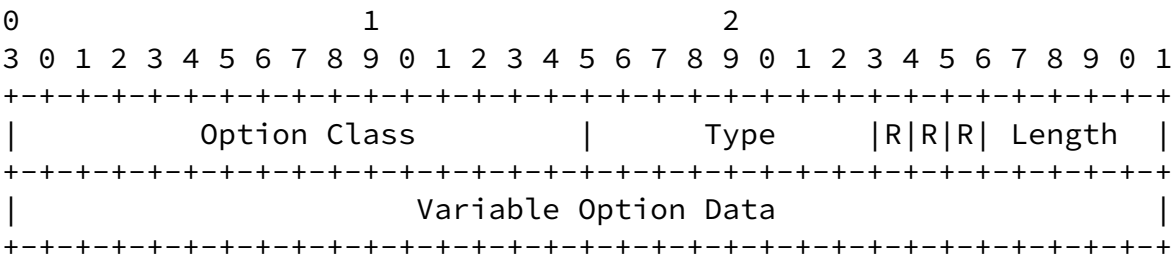


Figure 1: Geneve Option Format

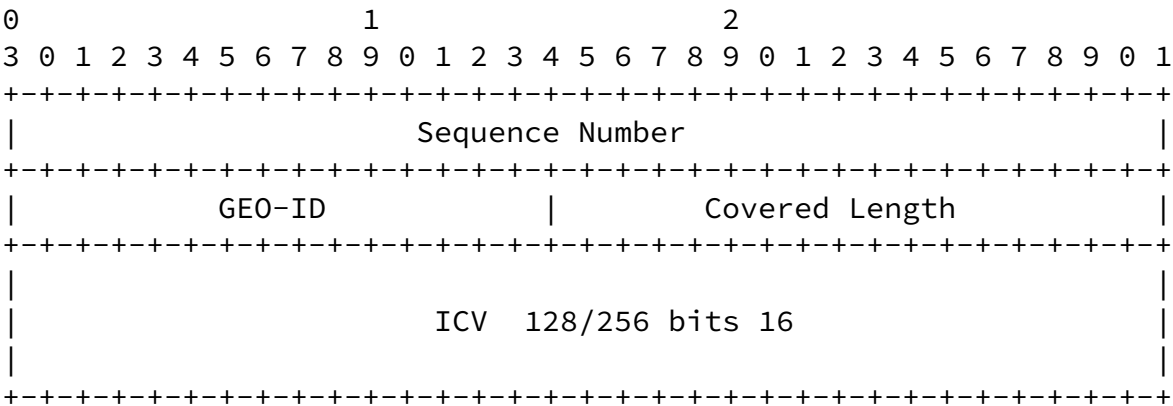
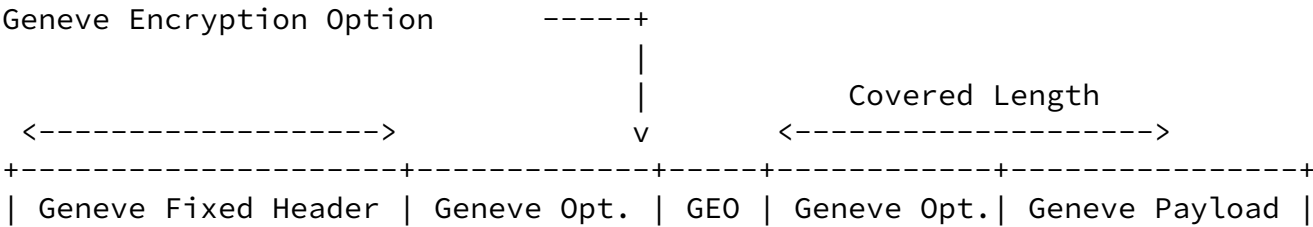


Figure 2: Geneve Encryption Data

4. GEO Processing

4.1. GEO Placement

[



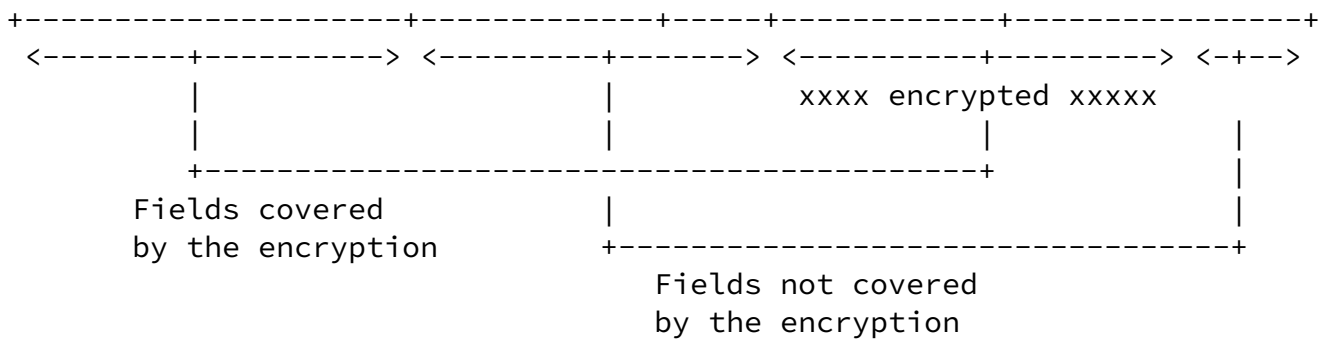


Figure 3: Geneve Encryption Options Placement

GEO is a termination Geneve Option. The encrypted Geneve Options and portion of the encrypted Geneve Payload are appended to the Geneve Header. They are not encoded as an Geneve Option.

## [5. IANA Considerations](#)

There are no IANA consideration for this document.

## [6. Security Considerations](#)

## [7. Acknowledgment](#)

## [8. References](#)

### [8.1. Normative References](#)

[I-D.ietf-ipsecme-rfc4307bis]

Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for IKEv2", [draft-ietf-ipsecme-rfc4307bis-18](#) (work in progress), March 2017.

[I-D.ietf-ipsecme-rfc7321bis]

Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", [draft-ietf-ipsecme-rfc7321bis-06](#) (work in progress), June 2017.

[I-D.ietf-nvo3-geneve]

Gross, J., Ganga, I., and T. Sridhar, "Geneve: Generic Network Virtualization Encapsulation", [draft-ietf-nvo3-geneve-04](#) (work in progress), March 2017.

[I-D.ietf-tls-dtls13]

Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", [draft-ietf-tls-dtls13-00](#) (work in progress), April 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

Migault

Expires December 29, 2017

[Page 4]

---

Internet-Draft

Geneve Header Encryption Option (GEO)

June 2017

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", [RFC 4106](#), DOI 10.17487/RFC4106, June 2005, <<http://www.rfc-editor.org/info/rfc4106>>.

[RFC4302] Kent, S., "IP Authentication Header", [RFC 4302](#), DOI 10.17487/RFC4302, December 2005, <<http://www.rfc-editor.org/info/rfc4302>>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", [RFC 4868](#), DOI 10.17487/RFC4868, May 2007, <<http://www.rfc-editor.org/info/rfc4868>>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", [RFC 6347](#), DOI 10.17487/RFC6347, January 2012, <<http://www.rfc-editor.org/info/rfc6347>>.

## [8.2.](#) Informative References

[I-D.ietf-nvo3-encap]

Boutros, S., Ganga, I., Garg, P., Manur, R., Mizrahi, T.,

Mozes, D., and E. Nordmark, "NV03 Encapsulation Considerations", [draft-ietf-nvo3-encap-00](#) (work in progress), June 2017.

[I-D.mglt-nvo3-geneve-security-architecture]

Migault, D., "Geneve Security Architecture", July 2017, <<https://tools.ietf.org/html/I-D.ietf-nvo3-geneve-security-architecture-00>>.

[I-D.mglt-nvo3-security-requirements]

Migault, D., "Geneve Security Requirements", July 2017, <<https://tools.ietf.org/html/I-D.mglt-nvo3-security-requirements-00>>.

[RFC7364] Narten, T., Ed., Gray, E., Ed., Black, D., Fang, L., Kreeger, L., and M. Napierala, "Problem Statement: Overlays for Network Virtualization", [RFC 7364](#), DOI 10.17487/RFC7364, October 2014, <<http://www.rfc-editor.org/info/rfc7364>>.

[RFC7539] Nir, Y. and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols", [RFC 7539](#), DOI 10.17487/RFC7539, May 2015, <<http://www.rfc-editor.org/info/rfc7539>>.

Migault

Expires December 29, 2017

[Page 5]

---

Internet-Draft      Geneve Header Encryption Option (GEO)

June 2017

Author's Address

Daniel Migault

Email: [daniel.migault@ericsson.com](mailto:daniel.migault@ericsson.com)

