

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

D. Migault  
June 27, 2017

Geneve Header Authentication Option (GAO)  
draft-mglt-nvo3-geneve-authentication-option-00

## Abstract

This document describes the Geneve Header Authentication Option (GAO). This option enables a Geneve element to authenticate 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>	Position versus DTLS/IPsec . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Scope of the GAO . . . . .	<a href="#">5</a>
<a href="#">5.</a>	Terminology . . . . .	<a href="#">6</a>
<a href="#">6.</a>	GAO Description . . . . .	<a href="#">6</a>
<a href="#">7.</a>	GAO Processing . . . . .	<a href="#">7</a>
<a href="#">7.1.</a>	GAO Placement . . . . .	<a href="#">7</a>
<a href="#">7.2.</a>	GSA Parameters . . . . .	<a href="#">8</a>
<a href="#">7.3.</a>	GAO Outbound Processing . . . . .	<a href="#">10</a>
<a href="#">7.3.1.</a>	Generating the Sequence Number . . . . .	<a href="#">10</a>
<a href="#">7.3.2.</a>	Generating a Covered Length . . . . .	<a href="#">11</a>
<a href="#">7.3.3.</a>	GAO Inbound Processing . . . . .	<a href="#">12</a>
<a href="#">8.</a>	IANA Considerations . . . . .	<a href="#">15</a>
<a href="#">9.</a>	Security Considerations . . . . .	<a href="#">15</a>
<a href="#">10.</a>	Acknowledgment . . . . .	<a href="#">15</a>
<a href="#">11.</a>	References . . . . .	<a href="#">15</a>
<a href="#">11.1.</a>	Normative References . . . . .	<a href="#">15</a>
<a href="#">11.2.</a>	Informative References . . . . .	<a href="#">16</a>
	Author's Address . . . . .	<a href="#">16</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

Geneve [[I-D.ietf-nvo3-geneve](#)] defines an overlay network that enables communications between tenants within a given virtual network. The Geneve overlay network enables these tenants to be distributed over a data center or multiple data centers. As multiple virtual networks share a common infrastructure, Geneve needs to isolate both communications between virtual networks as well as each virtual network address space [[RFC7364](#)].

The Geneve Header indicates the virtual network a communication belongs to with a Virtual Network Identifier (VNI). Geneve packets may be steered to the appropriated destination tenant through the destination switch based on that NVI value. In addition to the NVI,

the Geneve Header may carry additional metadata that impacts how the traffic could be steered to the destination tenant.

As stated by [[I-D.ietf-nvo3-encap](#)] and [[I-D.mglt-nvo3-security-requirements](#)], it is crucial that the

information of the Geneve Header remains protected and authenticated in order to prevent that traffic be delivered to the wrong tenant. Typically, without integrity check mechanisms, a one bit switch in the NVI results in such a wrong delivery. Such vulnerability is further increased by the use of UDP encapsulation that makes any application able to spoof packets.

This document addresses these issues by proposing a GAO which enables to authenticate the Geneve Header with a set of selected Geneve Options as well as a portion of inner packet (Geneve Payload) carried by the Geneve overlay network (Geneve Payload). In addition, GAO also prevent a Geneve Packet to be replayed by introducing an anti-replay mechanism. GAO does not provides encryption which is instead provided by [[I-D.mglt-nvo3-geneve-encryption-option](#)].

### 3. Position versus DTLS/IPsec

This section exposes the motivations for designing GAO rather than re-using existing security mechanisms such as DTLS or IPsec.

GAO provides integrity protection of a Geneve Packet, i.e. the Geneve Header, including a set of Geneve Options as well as a portion of the Geneve Payload.

As Geneve is encapsulated in UDP packet, DTLS is a natural candidate. Similarly IPsec/AH [[RFC4302](#)] defines an protocol to authenticate an IP packet. However relying on DTLS (or IPsec)/AH instead of a specific extension designed for Geneve comes with the following drawbacks:

- o Modern versions of DTLS [[I-D.ietf-tls-dtls13](#)] currently do not consider authentication-only. Instead the traffic is always encrypted. Encrypting the Geneve Header prevents on path Geneve elements to manage secured intra NVI communications. Typically when multiple intra NVI communications are multiplexed into a DTLS tunnel, a Geneve on path element will not be able to re-route some

traffic nor to appropriately prioritize flows or load balance them according to their NVI. On the other hand, DTLS1.2 [[RFC6347](#)] enabled authentication-only protection, and further cipher suite could be defined for DTLS1.3 in case there were a significant advantage in using DTLS to secure the Geneve communications. In case such cipher will not be available, currently defined end to end encryption would prevent providing information useful to manage the various intra-NVI communications. This information might be carried by lower layer such as UDP using port number for example. However, such alternatives clearly makes secure intra NVI communication unnecessarily too hard to manage, and so does

not encourage a secure deployment of these communications.  
Typically:

- \* Management of secure Geneve communications are reduces to management of UDP tunnel which ignores all motivations for designing Geneve. That is the ability to tag flows, as well as to carry states or metadata.
- \* Management complexity is increased with an additional binding between Geneve Header and port number for example. Not only a new binding is introduced, but as Geneve Headers and UDP source ports / destination ports have different spaces ranges, this makes such correspondence not straight forward to manage. Typically NVI are 24 bit long while source port are 16 bit long, this means that additional destination port may be used in order to benefit from the full NVI space.
- \* Increases the number of tunnels and the number of keying material as different Geneve Header needs to be transported in different UDP tunnel. The number of UDP tunnels may reach the number of different Geneve communications.
- o DTLS comes with a key exchange agreement, included as part of the DTLS protocol. In most cases, DTLS or TLS is used without any configurations by a (D)TLS client while the (D)TLS server has all the necessary authentication information, so the (D)TLS client can appropriately authenticate the (D)TLS server. In this case, for end-to-end authentication, authentication is performed by both Geneve NVEs which requires all of them to be appropriately

provisioned with the necessary authentication credentials. Management of these authentication credential is not trivial and is expected to be handled in addition of the security policies. In addition, the presence of such handshake protocol may introduce some latencies in a forwarding plane usually managed by an orchestrator. As a result, if DTLS would be used, a variant of DTLS without key exchange may rather be considered.

- o Geneve does not provide any standard way to inform whether a packet is authenticated or not. The current assigned port number for Geneve is 6081. In order to make possible for the receiving node to distinguish an unprotected Geneve Packet from a protected traffic, a new port should be defined.
- o The current use of TLS is usually based on a TLS client wishing to access a resource using TLS. In that case, the TLS client uses a specific port number. A server may also redirect the requests from a client that is non protected to a specific port which defines the protected version of that service. Such redirection

is usually performed when the service defines that resource has to be accessed using a secure channel. In addition, the redirection is performed by the application protocol. As a result, the security policies are usually quite simple that is, 1) security initiated by the client or 2) server enforces that all requested are secured. The case of Geneve overlay network considers instead the coexistence of protected and non protected traffic which would require some mechanisms to define and enforce security policies not yet part of DTLS.

- o DTLS usually protects the whole UDP payload. In our case, the protection of the Geneve Header only, for example, would require some further developments to the existing DTLS.
- o IPsec/AH prevents the creation of the Geneve overlay network. IPsec/AH has been defined for end-to-end IP communications. In the case of a Geneve Packet, the two ends are defined by the IP addresses of the Geneve Packet Outer IP Headers. These IP addresses are not necessarily the Geneve NVE, and could instead be those of an Geneve element that belong to the Geneve overlay network and in charge of steering the traffic to another Geneve overlay element. With IPsec/AH, the IP addresses could not be

modified, and the Geneve Packet will not be able to be steered across the Geneve overlay network. In this case IPsec/AH could be used for a hop-by-hop security. This would require each node of the Geneve Overlay network to be provisioned appropriately with the IPsec material which would come with significant management issues. In addition, this would not achieve a end-to-end security between the two ends of the Geneve tunnel.

- o IPsec/ESP may also be used without encryption. However, in this case, the port number would be protected, which would prevent Geneve element to redirect the traffic to a different Geneve element using a different port. Such constraint may prevent the overlay network to be operated as an overlay network, that is any on path Geneve element is able to redirect the traffic to another Geneve element that belongs to the overlay network.

#### 4. Scope of the GAO

The Geneve Header Authentication Option (GAO) expects to have the following properties:

- o Provides means to authenticate the Geneve Header, a selected associated set of options as well as part of the Geneve Payload.
- o Provides an anti-replay mechanism. This option does not encrypt any data and as such does not provide any privacy. When privacy

is expected, it can be enforced by the Geneve overlay network using GE0 ([\[I-D.mglt-nvo3-geneve-encryption-option\]](#)) as well as by the Tenant's System which may encrypt their communications using IPsec/ESP or TLS. The main purpose of the GAO is to provide means for the infrastructure to ensure that Geneve communications cannot be injected for example by modifying the NVI.

- o Provides authentication - at least in an orchestrated environment - to the two NVEs, but also to any appropriately configured on-path Geneve forwarding element.
- o Provides read access to the Geneve Header for any Geneve on path elements. This option is expected to enable Geneve communications to be secured, while benefiting from all the facilities provided by Geneve.

- o Provide the ability for on path Geneve forwarding elements to add Geneve Options on Geneve authenticated Packets without invalidating the GAO.
- o Provides means with some restrictions for an on-path element to add Geneve Option and authenticate that Geneve Option using a GAO.

## 5. Terminology

The terminology used in this document has been introduced in [\[I-D.mglt-nvo3-geneve-security-architecture\]](#).

## 6. GAO 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 GAO can simply be ignored by a NVE or a transit node. The GSP will prevent to accept a GAO 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 [\[I-D.ietf-ipsecme-rfc7321bis\]](#) AUTH\_HMAC\_SHA2\_256\_128 and AUTH\_HMAC\_SHA2\_512\_256. These algorithms are defined in [\[RFC4868\]](#) with a respective 16 and 32 byte ICV. As a result, the option length is expected to  $4 + 28 = 32$  bytes (resp.  $4 + 44 = 48$  bytes) which leads to 8 or 12 as the possible values for Length.

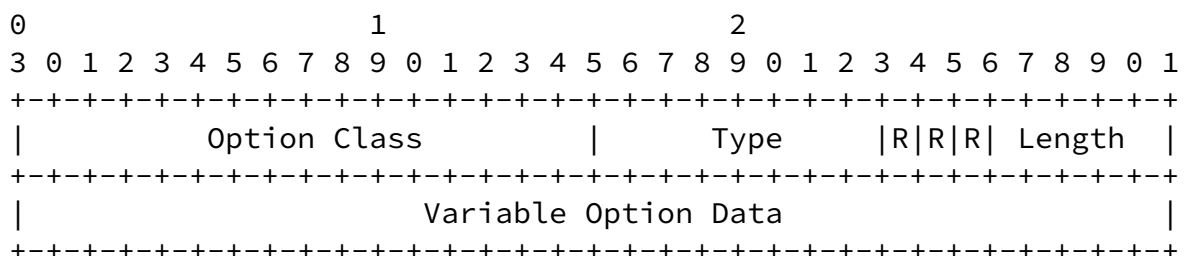


Figure 1: Geneve Option Format

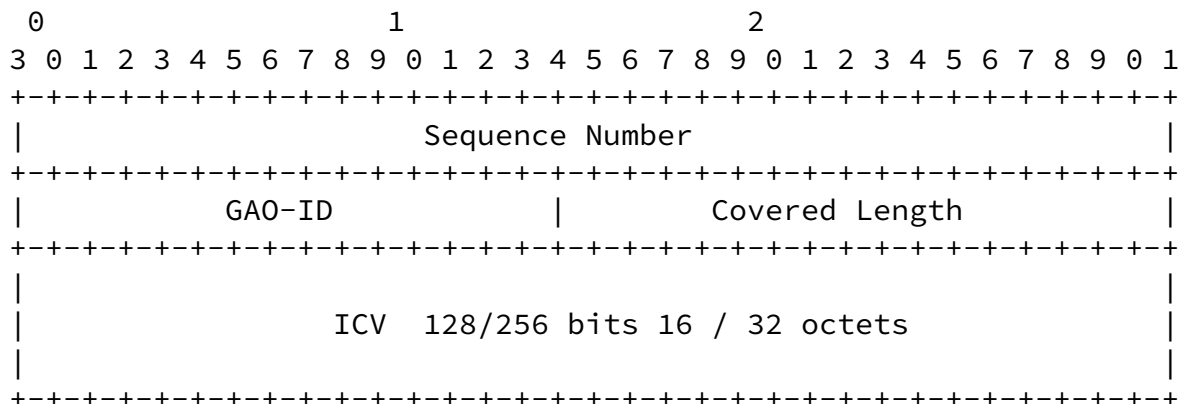


Figure 2: Geneve Authentication Data

- o Sequence Number (32 bits): indicates the Sequence number of the Geneve Header. When the SN is 32 bit long, the whole SN is indicated. When the SN is 64 bit long, only the 32 least significant bits are indicated.
- o GAO-ID (16 bits): indicates the identifier of the GAO. This identifier is useful to retrieve the GSA, with the necessary information to compute the GAO or to validate it.
- o Covered Length (16 bits): indicates in number of bytes following the GAO that are covered by the authentication.
- o ICV contains the HMAC value.

## [7. GAO Processing](#)

### [7.1. GAO Placement](#)

A GAO option covers the Geneve Header, the Geneve Options following the GAO as well as the Covered Length appended to the GAO. As a result, any on path (Geneve) element MUST leave the Geneve Fixed Header and the first Covered Length bytes after GAO unchanged.

GAO does not covers the Geneve Options placed between the Geneve



Fixed Header and the GAO. In addition, GAO does not cover the bytes located after the Covered Length.

Geneve Options that are expected to be updated by any Geneve forwarding elements MUST be located between the Geneve Fixed Header and the existing GAO.

When a Geneve Packet is received by a Geneve forwarding element and that element is expected to insert an additional Geneve Option, the Geneve forwarding element MUST NOT insert the Geneve Option in a area covered by a GAO. A safe way to proceed is that Geneve forwarding element that do not understand GAO MUST insert new Geneve Option right after the Geneve Fixed Header. This will result in having the Geneve Option before the existing GAO. When the Geneve forwarding element understand GAO it can consider the covered area by each GAO and place its new option in a non covered area.

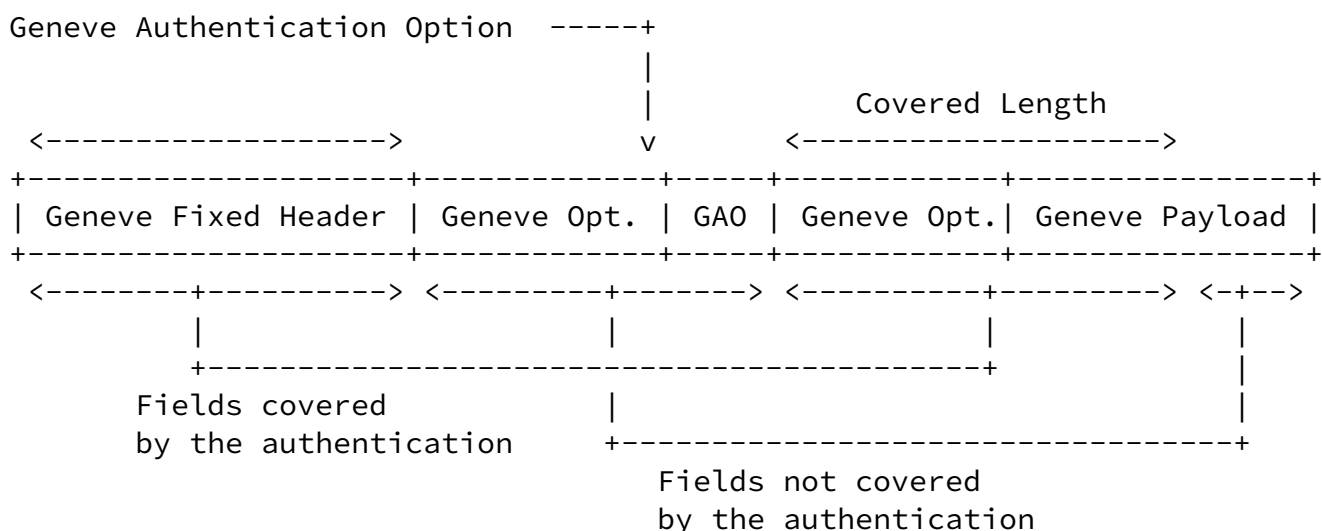


Figure 3: Geneve Authentication Options Placement

## 7.2. GSA Parameters

This section describes the parameters of the GAS necessary to compute or validate the GAO. These parameters are then latter used to described the processing.

- o GSO ID: The identifier of that GAO. This identifier is used to bind the GAO with the appropriated GSA. It is expected that GSA are uniquely identified on the receiver side. In case collision are supported, the implementation MUST be able to deterministically associate the GAO to the appropriated GSA for example by using IP addresses and UDP ports.

- o GSO Protocol: The security protocol associated with the Geneve Security Option. In our case the protocol is GAO.
- o GSO Authentication Algorithm: This document follows recommendations provided by [[I-D.ietf-ipsecme-rfc7321bis](#)] which recommends AUTH\_HMAC\_SHA2\_256\_128 and AUTH\_HMAC\_SHA2\_512\_256 defined in [[RFC4868](#)].
- o GSO Payload Covered Length: the length of the Geneve Payload covered by GAO. The expression of the length can be a number of bytes, but it may also be defined with an abstract designation. For example, a sending node may be willing to authenticate the Geneve Payload up to the ESP layer. In that case, the sending node will have to compute the corresponding Payload Covered Length. This value is only used by the sending node. The receiving node read that value from the GAO.
- o GSO Covered Geneve Options: Indicates the Geneve Options covered by the GAO. This indication is primarily necessary for the sending node and is derived from the Geneve Packet by the receiving node. It MUST be checked by the receiving node to validate the GSA. It might typically be expressed as a list of Geneve Options that needs to be covered by the authentication.
- o GSO Authentication Key: the shared secret necessary compute and validate the HMAC value generated by the Authentication Algorithm specified above.

In order to implement the anti replay mechanisms the following parameters are provided:

- o GSO Sequence Number Size: indicates the size of the SN. This document considers a 32 bit or a 64 bit length.
- o GSO Sequence Number: that designates the Sequence Number last sent or received packet.
- o GSO Anti Replay Window: that indicates the windows that defines out-of order packet or late packets versus a replayed Geneve Packet. Any Geneve Packet with a lower SN than GSO Sequence Number - Anti Replay Windows MUST be rejected.

In order to check the conformity with the GSP:

- o Selectors: The selectors are provided so the receiver can check the Geneve Packet protected by the GSO is conform to the GSP. In

other words a valid GSO is not sufficient for the Geneve Packet to be forwarded to the upper layers. Note that the Selectors MUST

match the Geneve Packet associated to the GSA before the GSO is built for outbound Packets. For inbound Geneve Packet the Selectors are those that correspond to the Geneve Packet after the GSO has been validated/decrypted. Selectors are mostly expected to be used by the GSA for incoming Geneve Packet, in order to check the GSA is conform with its GSP.

- o GSA Life time:

### [7.3.](#) GAO Outbound Processing

Upon receiving a Geneve Packet, the Geneve Security Module performs a GSP DB look up to determine if any security action is required. If the security action is DISCARD, the Geneve Packet is discarded. If the security action is BYPASS, the Geneve Packet is sent to the lower layers for the outer encapsulation without any additional security consideration. If the action is SECURE, the GSP returns the list of GSAs that need to be applied. The list is an ordered list, and the Geneve Security Module performs these GSAs in the received order. (See [[I-D.mglt-nvo3-geneve-security-architecture](#)] for more information.)

When a list of GSAs is provided, it is crucial that the implementation updates the Selectors of the further GSAs according to the actions undertaken by the previous GSAs. In most cases, a GSA results in the addition of GSO. The Selectors of the next GSA MUST consider this new GSO, in the Selectors.

The outbound processing consists in the following actions:

1. Generating the Sequence Number
2. Generating a Covered Length
3. Generating the ICV
4. Building the GAO
5. Building the output Geneve Packet

### [7.3.1.](#) Generating the Sequence Number

The Sequence Number is used to prevent anti replay. The Sequence Number is any number strictly greater than the current value of the GSO Sequence Number mentioned in the GSA.

The size of the GSO Sequence Number is designated by the GSO Sequence Number Size. The GSO Sequence Number can be a 32 bit or 64 bit

number. When the limit or the GSO Sequence number has been reached, the GSA MUST be renewed. In other words, no re-initialization nor rolling mechanisms are expected for the GSO Sequence Number. The Geneve Elements need to take the necessary actions in order to generate GSAs before the limit of the GSO Sequence Number is reached.

The new value of the GSO Sequence Number replaces the former GSO Sequence Number in the GSA.

### [7.3.2.](#) Generating a Covered Length

The Covered Length describes the number of bytes of the Geneve Packet that are located after the GAO and authenticated by GAO.

The Covered Length includes Geneve Options that are covered by the authentication designated by the GSO Covered Geneve Options as well as a portion of the Geneve Payload designated by the GSO Payload Covered Length.

The covered Geneve Options MUST be immutable, and any on-path Geneve element MUST NOT change any of the Geneve Options covered by GAO. The covered Options MAY be agreed between the two Geneve element, however, by default, it is expected that the sending node will include any immutable Geneve Option. The agreement of the covered Geneve Options is not necessary to validate the GAO. In fact the position of the GAO in the Geneve Packet indicates deterministically the covered Geneve Options. However, Geneve Options that are immutable while not being covered by the GAO will be considered suspicious and as such SHOULD be rejected by the Geneve Security Module of the receiving node. This Geneve Option could have been inserted as well as modified. Of course some Geneve Security Module MAY also specify a list of immutable Geneve Option that are not

expected to be covered. In that case such options MUST NOT be removed by the Geneve Security Module.

Overall, the covered Geneve Options is determined by the sending node. In addition that Geneve Options may have varying size, the contribution of the Covered Length is likely to vary for each Geneve Packet.

Similarly, the contribution of the Covered Length by the Geneve Payload is also likely to vary for each Geneve Packet. More specifically, it is more likely that a GSA defines the layers of the Geneve Payload that needs to be authenticated instead of a number of bytes. For example, a GSA may indicate that the Geneve Payload may be covered up to the ESP or (D)TLS layer. In addition, the GSA may also indicate an upper bound value for the Covered Length which could be imposed by hardware or computing restrictions. As a result, the

contribution of the Geneve Payload is determined by the sending node and evaluated for each Geneve Packet.

#### [7.3.2.1.](#) Generating the ICV

The ICV results from applying the GSO Authentication Algorithm with the GSO Authentication Key to the appropriated data.

The appropriated data is build by concatenating the initial string "geneve authentication option" with the Geneve Fixed Header, the GSO Sequence Number, the GSO-ID, the GSO Covered Length, the covered Geneve options as well as the covered part of the Geneve Payload.

All fields of the Geneve Fixed Header are considered, including the Rsv and Reserved fields. It is important to understand that these fields are expected to remain immutable fields.

#### [7.3.2.2.](#) Building the GAO

The GAO is built by concatenating the 32 least significant bits of the GSO Sequence Number, the GAO-ID, the Covered Length and the generated ICV.

#### [7.3.2.3.](#) Building the output Geneve Packet

The GAO is placed before all covered Geneve Options, followed by the Geneve Payload. A Geneve Option that is not covered by the GAO MUST NOT be placed after the GAO. The Geneve Options covered by the GAO MUST remain in the same order as the order considered for generating the ICV. A Geneve Option covered by the GAO MUST NOT be located before the GAO. In addition, a Geneve Element MUST NOT change any bit located after the GAO that is covered by the GAO.

The generated Geneve Packet is then forwarded to the Outer Tunnel encapsulation.

### [7.3.3.](#) GAO Inbound Processing

Upon receiving a Geneve Packet, the receiving Geneve element determines the Geneve Packet is neither associated with a DISCARD nor with a BYPASS policy, and as such is expected to be SECURED – see [\[I-D.mglt-nvo3-geneve-security-architecture\]](#).

When the Geneve Security Module finds a GAO, the inbound processing consists in the following actions:

1. Computing the Sequence Number

2. Validate the ICV
3. Apply the anti-replay protection
4. Remove the GAO from the Geneve Packet
5. GSP Validation

#### [7.3.3.1.](#) Computing the Sequence Number

When the GSO Sequence Number Size indicates the GSO Sequence Number is coded over 32 bits, the Sequence Number is as indicated in the GAO.

When the GSO Sequence Number Size indicates the GSO Sequence Number is coded over 64 bits, the receiving node needs to evaluate the value of the 32 most significant bits. If the Sequence Number is lower than the 32 least significant bits of the GSO Sequence Number, the

receiving node will assume the 32 most significant bits of the Sequence Number are the most significant bits of the GSO Sequence incremented by one. The Sequence Number is evaluated as the combination of its 32 most significant bits and the 32 least significant bits indicated in the GAO.

In case it is not possible to increment these 32 most significant bits, the Sequence Number is considered out of the limit and the Geneve Packet is rejected.

It is worth noting that if the Sequence number MUST NOT be incremented by several order of the most significant bits.

#### [7.3.3.2.](#) ICV Validation

To validate the ICV, the receiving node computes the ICV and compares the computed value with the value carried by the GAO. If the two values match the ICV is validated. In case of mismatch, the Geneve Packet is rejected.

The ICV results from applying the GSO Authentication Algorithm with the GSO Authentication Key to the appropriated data.

The appropriated data is build by concatenating the initial string "geneve authentication option" with the Geneve Fixed Header, the GSO Sequence Number, the GSO-ID, the Covered Length, the covered Geneve data.

All elements are read from the Geneve Fixed Header or the GAO and the covered data is read as the number of bytes indicated by the Covered Length value of the GAO that follow the GAO.

#### [7.3.3.3.](#) Anti Replay Protection

The receiving node reads the Sequence Number and Compare it with the GSO Sequence Number stored in the GSA. The difference Delta is evaluated by computing GSO Sequence Number - Sequence Number.

If Delta is greater than GSO Anti Replay Window, the Geneve Packet is

rejected.

If Delta is strictly negative, the GSO Sequence Number is updated with the value of the Sequence Number.

#### [7.3.3.4.](#) GAO Removal

Once the ICV protection has been verified as well as the anti replay protection, the GAO is removed from the Geneve Packet. The removal of the Option occurs after the UDP decapsulation, thus there is no impact on the Geneve Packet, and, for example, no length needs to be adjusted.

#### [7.3.3.5.](#) GSP Validation

GSP Validation validates a given GAO is conform to the expected GSP. This means that when the GAO has been removed, the resulting Geneve Packet is matched against the GSP DB in order to validate the resulting Geneve Packet is associated to the GSA. Such verification is performed by checking the GSO Selectors.

The Geneve Security Module also checks that the expected part of the Geneve Packet have been covered as expected. This includes the Geneve Options as well as the Geneve Payload Length. In case a mismatch is detected the Geneve Packet MUST be rejected.

Some implementations MAY perform additional checks or transformations. For example, some implementation, unless specified or agreed otherwise, SHOULD remove the immutable Geneve Options that are not covered by the validation.

Once validation is completed, the Geneve Packet is forwarded to the Geneve Layer.

## [8.](#) IANA Considerations

There are no IANA consideration for this document.



## [9.](#) Security Considerations

## [10.](#) Acknowledgment

## [11.](#) References

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

[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>>.

[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>>.

## 11.2. 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-encryption-option]

Migault, D., "Geneve Encryption Option", July 2017, <<https://tools.ietf.org/html/I-D.ietf-nvo3-geneve-encryption-option-00>>.

[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>>.

## Author's Address

Daniel Migault

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

