IPsecme
Internet-Draft
Intended status: Standards Track
Expires: 17 September 2025

D. Migault
Ericsson
M. Hatami
Concordia University
D. Liu
S. Preda
Ericsson
W. Atwood
S. C迪spedes
Concordia University
T. Guggemos
LMU
D. Schinazi
Google LLC
16 March 2025

Internet Key Exchange version 2 (IKEv2) extension for Header Compression Profile (HCP)
draft-ietf-ipsecme-ikev2-diet-esp-extension-05

Abstract

This document describes an IKEv2 extension for Header Compression to agree on Attributes for Rule Generation. This extension defines the necessary registries for the ESP Header Compression Profile (EHCP) Diet-ESP.

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 https://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 17 September 2025.

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Introduction

The ESP Header Compression Profile (EHCP) [I-D.ietf-ipsecme-diet-esp] minimizes the overhead associated with ESP by compressing both the ESP header and additional fields within the secured packet. EHCP utilizes Attributes for Rule Generation (AfRG) that are specified for each Security Association (SA). Certain AfRG have already been established during the SA negotiation process through IKEv2. This extension facilitates the agreement on the remaining AfRG through IKEv2.

3. Protocol Overview

As illustrated in Figure 1, an initiator intending to utilize the Header Compression Profile (HCP) informs its peer by sending a HCP_PROPOSAL Notify Payload during the IKE_AUTH and CREATE_CHILD_SA exchanges. The HCP_PROPOSAL includes a list of Proposals, each comprising an EHCP Name along with a set of AfRG [I-D.ietf-ipsecme-diet-esp]. Any AfRG for which the initiator wishes to specify no limitations SHOULD be excluded, i.e., an AfRG is only sent if the sending peer wants the receiving peer to select a subset of the available values. A given AfRG MAY be repeated with different values in order to provide a list of acceptable values. A range of possible AfRG values MAY be indicated as well.

If a Proposal contains an unknown HCP Name, or any AfRG in a Proposal is unknown, then the entire Proposal must be discarded by the responder. If none of the received Proposals are deemed acceptable, the responder MAY choose to discard the HCP_PROPOSAL Notify Payload. Nevertheless, it is anticipated that the responder will provide an explanation for rejecting all HCP Proposals. If the reason pertains to an AfRG with an unacceptable value, the responder SHOULD reply with a NO_PROPOSAL_CHOSEN Notify Payload.

Conversely, if the receiver identifies a suitable Proposal, it will respond with an HCP_PROPOSAL Notify Payload that includes the chosen Proposal. In cases where the AfRG was not explicitly stated, the responder will provide the AfRG unless it defaults to a standard value. Each AfRG MUST NOT be mentioned more than one time. When multiple values are provided for a specific AfRG (either multiple values being provided or via a range of acceptable values), the responder MUST NOT provide more than one value. The Proposal MUST NOT contain any range of AfRG.

Upon receipt of an NO_PROPOSAL_CHOSEN Notify Payload, the initiator has the option to restart the CREATE_CHILD_SA exchange.

When the initiator receives the HCP_PROPOSAL_CHOSEN Notify Payload, it will evaluate the Proposal to ensure that it aligns with the initial proposal and adheres to its policies prior to executing the HCP.

```
Initiator                          Responder
-------------------------------------------------------------------
HDR, SA, KEi, Ni -->
                           <-- HDR, SA, KEr, Nr
HDR, SK {IDi, AUTH,
     SA, TSi, TSr,
     N(HCP_PROPOSAL
         Proposal_ID=1, HCP Name="Diet-ESP"
           AfRG_a
           ...
           AfRG_i
         ...
         Proposal_ID=2, HCP Name="Diet-ESP"
           AfRG_a
           ...
           AfRG_j)
                           <-- HDR, SK {IDr, AUTH,
                                    SA, TSi, TSr,
                                    N(HCP_PROPOSAL
                                      Proposal_ID=2, HCP Name="Diet-ESP"
                                        AfRG_a
                                        ...
                                        AfRG_j,
                                        AfRG_k,
                                        ...
                                        AfRG_u)
```

Figure 1: The parameters for Diet-ESP have been established through the HCP_PROPOSAL_CHOSEN Notify exchange. In this instance, the responder has opted for the second Proposal, which includes the specified AfRG. Any absent AfRG will default to its predetermined values.

4. HCP_PROPOSAL Notify Payload

Figure 2 describes the HCP_PROPOSAL Notify Payload.

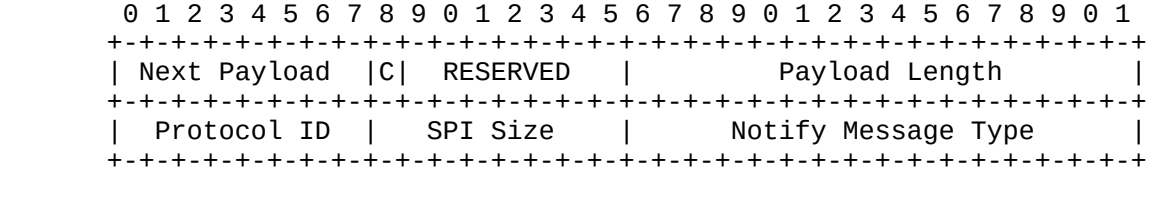

Figure 2: Notify Payload

The fields Next Payload, Critical Bit, RESERVED, and Payload Length are defined in section 3.10 of [RFC7296].

Protocol ID (1 octet): set to zero.

SPI Size (1 octet): set to zero.

Notify Message Type (2 octets): Specifies the type of notification message. It is set to TBA1 for HCP_PROPOSAL_CHOSEN.

When sent by the Initiator, the HCP_PROPOSAL Notify Payload contains a list of Proposals described in Figure 3. When sent by the responder the HCP_PROPOSAL Notify Payload contains a single Payload described in Figure 3.

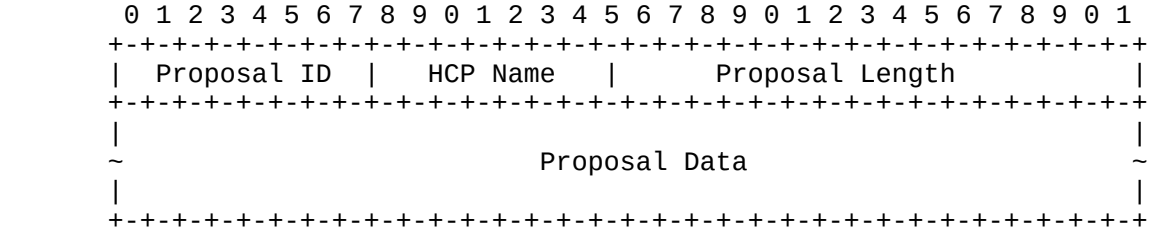

Figure 3: Proposal

Proposal ID (1 octet): The number identifying the Proposal.

EHCP Name (1 octet): The identifier of the EHCP Name (see Table 2).

Proposal Length (2 octets): The length in octets of the Proposal Data.

Proposal Data: A Proposal contains a set of parameters that are represented via Transform Attribute format [RFC7296], Section 3.3.5 and detailed further as described in Section 5.

5. Attributes for Rule Generation

Attributes for Rule Generation (AfRG) follow the same format as the Transform Attribute [RFC7296], Section 3.3.5 copied for convenience in Figure 4.

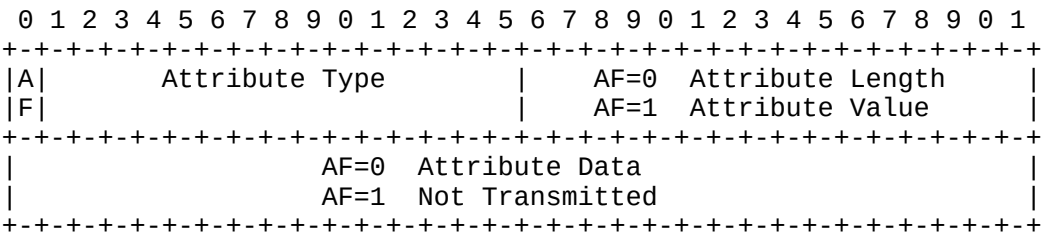

Figure 4: Transform Attribute Payload

There exist two categories of attributes: 1) generic attributes, which are applicable across all HCPs and serve to enhance the representation of a combination of AfRGs, and 2) AfRGs that are tailored to a particular HCP and possess a distinct value.

5.1. Generic Attributes

This specification defines range_afrg_proposal as a Generic Attribute for Rule Generation to specify that a given AfRG can be selected within a range of values.

* Designation: range_afrg_proposal

* Attribute Format: 0

* Attribute Data: Let AfRG_min and AfRG_max be the minimum and maximum values of the proposed range, expressed following the Transform Attribute Payload format. The corresponding Attribute Data is the concatenation of AfRG_min and AfRG_max.

To avoid ambiguity, it is explicitly required that both AfRG_min and AfRG_max refer to the same type of parameter and that they are processed as attributes with values defining the minimum and maximum of the range. This ensures consistent interpretation during negotiation and compression.

The figure below illustrates a Proposal for a compressed SPI between 6 and 8 bit long. SPI are compressed by sending LSB, so in our case AfRG_min is an esp_spi_lsb AfRG set to 6 and AfRG_max is a esp_spi_lsb set to 8. The esp_spi_lsb AfRG is detailed in the Diet-ESP EHCP Section 7 and is a 2 byte length Attribute. The resulting range proposal is expressed via the combination of the range_afrg_proposal and AfRG_min and AfRG_max.

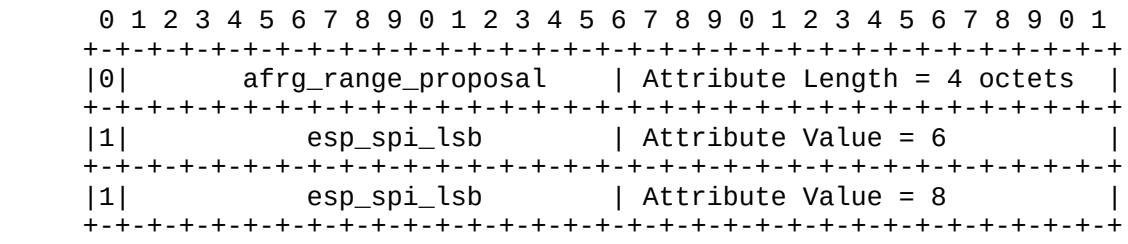

Figure 5: Illustration of the use of the range_afrg_proposal defining a range of SPI length

6. Registering a Header Compression Profile

An HCP needs to register an HCP Name taken from Table 2 in Section 8.3, the specification that describes the operations of the EHCP, as well as the different AfRG. For each AfRG, the corresponding Attribute Type, the AF value, the Attribute Data or Attribute Value and the Default Value MUST be specified.

7. AfRG for the Diet-ESP HCP

This section defines the code points that are needed to agree on the AfRG between two IKEv2 peers as described in Section 6.

* HCP Name: "Diet-ESP" as specified in Table 2, Section 8.3.

* Specification : [I-D.ietf-ipsecme-diet-esp]

The following Attributes for Rule Generation are defined:

DSCP Compression/Decompression Action (CDA)

* Designation: dscp_cda

* Attribute Format: 1

* Attribute Value: DSCP CDA takes discrete values coded over one byte as described in DSCP CDA Value Registry (Table 4 in Section 8.5.1)

* Default Value: the default value is set to "not_compressed"

ECN Compression/Decompression Action (CDA)

* Designation: ecn_cda

* Attribute Format: 1

* Attribute Value: ECN CDA takes discrete values coded over one byte as described in the ECN CDA Value Registry (Table 5 in Section 8.5.2)

* Default Value: the default value is set to "not_compressed"

Flow Label Compression/Decompression Action (CDA)

* Designation: flow_label_cda

* Attribute Format: 1

* Attribute Value: Flow Label CDA takes discrete values coded over one byte as described in the Flow Label CDA Value Registry (Table 6 in Section 8.5.3)

* Default Value: the default value is set to "not_compressed"

ESP Byte Alignment

* Designation: alignment

* Attribute Format: 1

* Attribute Value: Byte Alignment takes discrete values coded over one byte as described in the Bit Alignment Value Registry (Table 7 in Section 8.5.4)

* Default Value: the default value is set to "64 bit", which corresponds to the standard IPv6 bit alignment. The default value of 64 bit in this specification refers to the bit alignment used for Diet-ESP compression operations and does not override or contradict the alignment requirements of RFC 4303. Instead, the alignment specified here ensures compatibility with the SCHC compression framework, which is designed to operate efficiently in constrained networks.

ESP Trailer

* Designation: esp_trailer

* Attribute Format: 1

* Attribute Value: ESP Trailer takes discrete values coded over one byte as described in the Bit Alignment Value Registry (Table 8 in Section 8.6)

* Default Value: the default value is set to "Optional", which enables the ESP Trailer to be compressed.

Security Parameter Index (SPI) Least Significant Bits (LSB)

* Designation: esp_spi_lsb

* Attribute Format: 1

* Attribute Value: SPI LSB designates the number of bits that are provided to infer the SPI. This number is between 0 and 32.

* Default Value: the default value is 32, which is the size of the standard SPI in the standard ESP.

Sequence Number (SN) Least Significant Bits (LSB)

* Designation: esp_sn_lsb

* Attribute Format: 1

* Attribute Value: SN LSB designates the number of bits that are provided to infer the SPI. This number is between 0 and 32.

* Default Value: the default value is 32, which is the size of the standard SN in the standard ESP.

8. IANA Considerations

8.1. Registration of IKEv2 Notify Message Types

IANA has allocated one value in the "IKEv2 Notify Message Types - Status Types" registry:

Value	Notify Messages - Status Types
TBA1	HCP_PROPOSAL

This specification requests the IANA to create a Header Compression Profile registry (see Section 8.3), as well as the necessary registries for the ESP Header Compression Profile Diet-ESP, that is the Attributes for Rule Generation (see Section 8.4) as well as, when required, the complementary specific AfRG Values associated with each AfRG (see Section 8.5).

Note that the term "Header Compression Profile" reflects the purpose of the registry, which is to define profiles for ESP header compression using the Diet-ESP methodology. While the registry is

managed and utilized exclusively by IKEv2 for negotiating compression parameters, its scope is limited to ESP header compression and does not extend to IKEv2 itself.

All registries are "Specification Required".

8.2. Registry for Generic Attributes for Rule Generation

Registry for Generic Attributes for Rule Generation. When Associated Data is set to YES, the AF bit of the corresponding Transform Attribute Payload is set to 0; otherwise it is set to 1. The AfRG Code Point mentioned here MUST NOT be reused by any Registries associated with any Profile and is shared by all profiles.

AfRG Code Point	Full Name	Designation	Attribute Format	Reference
65535	RANGE AfRG	range_afrg_proposal	0	ThisRFC

Table 1

Each entry in the range is represented by two attributes (AfRG_min and AfRG_max), both following the 2-byte Attribute Type format specified in [RFC7296]. This ensures clarity and compatibility in all implementations.

8.3. Registry for IKEv2 Header Compression Profile

Value (1 Byte)	Designation	Reference
0	Diet-ESP	ThisRFC
1-255	unallocated	-

Table 2

8.4. Registry for Diet-ESP Attributes for Rule Generation

Registry for Attributes for Rule Generation for the ESP Header Compression Profile Diet-ESP. When Associated Data is set to YES, the AF bit of the corresponding Transform Attribute Payload is set to 0; otherwise it is set to 1.

The Diet-ESP Attributes for Rule Generation registry specifies six AfRG parameters explicitly defined for Diet-ESP that are not part of the standard IKEv2 negotiation process. These attributes are required for implementing the Diet-ESP Header Compression Profile. The remaining attributes referenced in [RFC7296], [RFC4301], and related drafts (e.g., DSCP values) are already defined and negotiated during the creation of the CHILD SA.

AfRG Code Point	Full Name	Designation	Attribute Format	Reference
0	DSCP CDA	dscp_cda	1	ThisRFC
1	ECN CDA	ecn_cda	1	ThisRFC
2	Flow Label CDA	flow_label_cda	1	ThisRFC
3	Alignment	alignment	1	ThisRFC
4	SPI LSB	esp_spi_lsb	1	ThisRFC
5	SN LSB	esp_spi_sn	1	ThisRFC
6 - 2^16-2	unallocated	-	-	-

Table 3

8.5. Registries for the Values of Diet-ESP Attributes for Rule Generation

8.5.1. DSCP CDA Value Registry

Value	Designation	Reference
0	not_compressed	ThisRFC
1	lower	ThisRFC
2	sa	ThisRFC
3-255	unallocated	-

Table 4

8.5.2. ECN CDA Value Registry

Value	Designation	Reference
0	not_compressed	ThisRFC
1	lower	ThisRFC
2-255	unallocated	-

Table 5

8.5.3. Flow Label CDA Value Registry

Value	Designation	Reference
0	not_compressed	ThisRFC
1	lower	ThisRFC
2	generated	ThisRFC
3	zero	ThisRFC
4-255	unallocated	-

Table 6

8.5.4. ESP Byte Alignment

Value	Designation	Reference
0	8 bit	ThisRFC
1	16 bit	ThisRFC
2	32 bit	ThisRFC
3	64 bit	ThisRFC
4-255	unallocated	-

Table 7

8.6. ESP Trailer

Value	Designation	Reference
0	Mandatory	ThisRFC
1	Optional	ThisRFC
2-255	unallocated	-

Table 8

9. Security Considerations

The protocol defined in this document does not modify IKEv2.

Proposals may be expressed in various ways and a proposal may be expressed in a specific way so that its treatment overloads the receiver. The receiver needs to consider aborting the exchange when too much resource is required.

10. Acknowledgements

The authors extend their gratitude to Samita Chakrabart, Tero Kivinen, Michael Richarson and Valery Smyslov for their long time support. The authors would like to acknowledge the support from Mitacs through the Mitacs Accelerate program.

11. Normative References

[I-D.ietf-ipsecme-diet-esp] Migault, D., Hatami, M., C迪spedes, S., Atwood, J. W., Liu, D., Guggemos, T., Bormann, C., and D. Schinazi, "ESP Header Compression with Diet-ESP", Work in Progress, Internet-Draft, draft-ietf-ipsecme-diet-esp-06, 16 March 2025, <https://datatracker.ietf.org/api/v1/doc/document/draft-ietf-ipsecme-diet-esp/>.

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

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

Daniel Migault
Ericsson
Email: daniel.migault@ericsson.com

Maryam Hatami
Concordia University
Email: maryam.hatami@mail.concordia.ca

Daiying Liu
Ericsson
Email: harold.liu@ericsson.com

Stere Preda
Ericsson
Email: stere.preda@ericsson.com

J. William Atwood
Concordia University
Email: william.atwood@concordia.ca

Sandra C迪spedes
Concordia University
Email: sandra.cespedes@concordia.ca

Tobias Guggemos
LMU
Email: guggemos@nm.ifi.lmu.de

David Schinazi
Google LLC
Email: dschinazi.ietf@gmail.com