Workgroup: IPsecme
Internet-Draft:
draft-mglt-ipsecme-ikev2-diet-esp-extension-03
Published: 28 June 2023
Intended Status: Standards Track
Expires: 30 December 2023
Authors: D. Migault Ericsson
T. Guggemos LMU
D. Schinazi Google LLC

# Internet Key Exchange version 2 (IKEv2) extension for the ESP Header Compression (EHC)

## Abstract

This document describes an IKEv2 extension of for the ESP Header Compression (EHC) to agree on a specific ESP Header Compression (EHC) Context.

## 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 30 December 2023.

**Table of Contents**


1. Requirements notation
2. Introduction
3. Protocol Overview
4. EHC_SUPPORTED and EHC_UNACCEPTABLE_PARAMETER Notify Payload
5. Parameters
6. IANA section
7. References
   7.1. Normative References
   7.2. Informative References

Authors' Addresses


## 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

ESP Header Compression (EHC) [I-D.mglt-ipsecme-diet-esp] reduces the ESP overhead by compressing the ESP and other fields of the protected packet. EHC takes an EHC Context defined for each Security Association (SA). The EHC Context contains some parameters that have already been agreed during the negotiation of the SA via IKEv2. This extension enable the remaining parameters to be agreed via IKEv2.

## 3. Protocol Overview

As depicted in Figure 1, an initiator willing to apply EHC notify its peer with a EHC_SUPPORTED Notify Payload in its IKE_AUTH and CREATE_CHILD_SA exchange. The EHC_SUPPORTED contains a list of Proposals payload which each contains some Parameter payloads that describes the acceptable values for the parameters of the EHC Context. Multiple Proposals are especially expected to enable multiple ECH Context to be defined and enable the initiator that organize subsets of parameters.

A Proposal is associated to an EHC Context specified with the ehc_context_id parameter. A Proposal MAY have multiple ehc_context_id parameters. In the absence of ehc_context_id parameter, the ehc_context_id parameter is assumed to "Diet-ESP". A Proposal contains all acceptable values associated to the EHC Context designated by ehc_context_id (including the default value). When unspecified, the initiator indicates that all possible values are acceptable. The absence of Proposal is considered as an empty Proposal. An empty Proposal is considered as a Proposal associated

to the Diet-ESP EHC Context with where the parameters of the EHC Context can take any value. Figure 1 depicts the example where where n Proposal are sent, each containing a set of parameters.

Upon receiving a EHC_SUPPORTED from the initiator, the responder look the various Proposals. In the absence of Proposal, the responder assumes the ehc_context_id parameter is set to "Diet-ESP" with all possible values for the Diet-ESP EHC being acceptable to the initiator. If one or more Proposal are present. For each Proposal, the responder looks for the ehc_context_id parameter. In the absence of such attribute the responder assumes ehc_context_id is set to "Diet-ESP". If the presence of one or multiple ehc_context_id parameters, the responder ignores the values it does not support. When an ehc_context_id is supported, the responder looks for the parameters associated to the EHC Context designated by ehc_context_id. The responder MUST understand the parameter associated to the EHC Context it supports, and ignore those of EHC Context it does not support. Depending on the responder's policy the responder keeps the acceptable Proposal and discard those that are not.

From the set of acceptable proposal, the responder determine a proper EHC Context. The responder MUST explicitly indicate the ehc_context_id parameter with all parameter associated to that EHC Context.

If none of the ehc_context_id parameter provided are supported, the responder SHOULD send a EHC_UNSUPPORTED_PARAMETER. Figure 1 depicts the responder selecting an EHC Context set designated as "Diet-ESP" with the selected_param_a, ..., selected_param_m.

```
Initiator                          Responder
-------------------------------------------------------------------
HDR, SA, KEi, Ni -->
                              <-- HDR, SA, KEr, Nr
HDR, SK {IDi, AUTH,
     SA, TSi, TSr,
     N(EHC_SUPPORTED
         Proposal_1
           param_a
           ...
           param_i
         ...
         Proposal_n
           param_a
           ...
           param_j)
                              <-- HDR, SK {IDr, AUTH,
                                       SA, TSi, TSr,
                                       N(EHC_SUPPORTED
                                         ehc_context_id = "Diet-ESP"
                                         selected_param_a
                                         ...
                                         selected_param_m )
```

Figure 1: Diet-ESP parameters agreed via the EHC_SUPPORTED Notify exchange

Currently, Diet-ESP [I-D.mglt-ipsecme-diet-esp] is the only defined EHC Context, but additional EHC Context may be defined in the future.

[I-D.mglt-ipsecme-diet-esp] defines the parameters associated to the Diet-ESP EHC Context. Figure 2 describes the parameters agreed by the EHC_SUPPORTED for Diet-ESP are mentioned below with the possible values and the default values indicated with an (*).

| EHC Context | Possible Values |
|---|---|
| ehc_context_id | "Diet ESP"* |
| alignment | "8 bit", "32 bit"* |
| esp_spi_lsb | 0, 1, 2, 3, 4* |
| esp_sn_lsb | 0, 1, 2, 3, 4* |
| ts_flow_label | True*, False |

Figure 2: Diet-ESP parameters agreed via the EHC_SUPPORTED Notify exchange

## 4. EHC_SUPPORTED and EHC_UNACCEPTABLE_PARAMETER Notify Payload

Figure 3 describes the EHC_SUPPORTED and EHC_UNACCEPTABLE_PARAMETER Notify Payload.

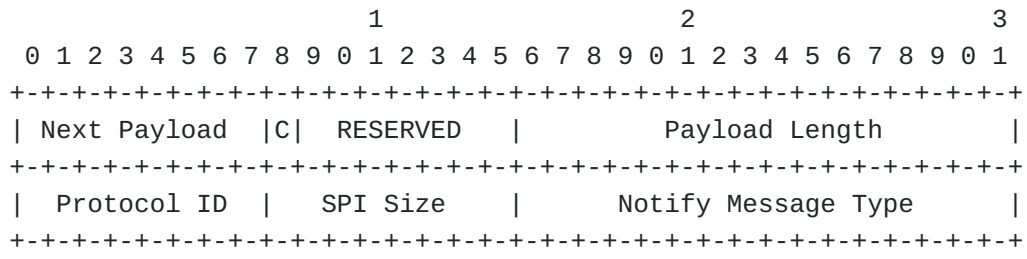


Figure 3: Notify Payload

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 EHC_SUPPORTED and TBA2 for EHC_UNACCEPTABLE_PARAMETER

When sent by the Initiator, the initiator contains a list of Proposal payload described by Figure 4.

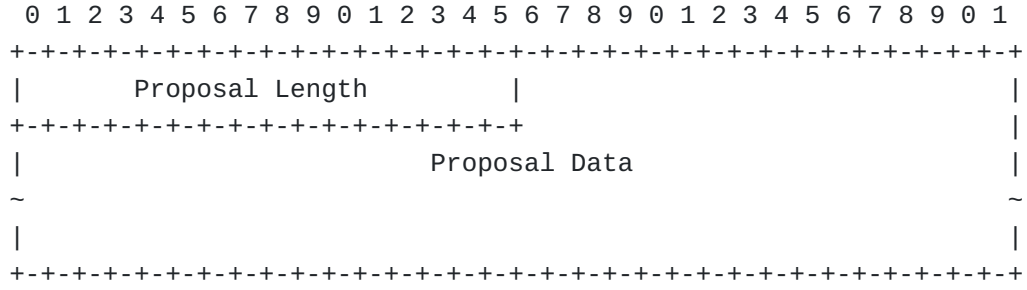


Figure 4: Proposal Payload

**Proposal Length (2 octets):** The length in octet 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 in as described in Section 5.

## 5. Parameters

Parameters follow the same format as the Transform Attribute [RFC7296], Section 3.3.5 reminded for convenience by

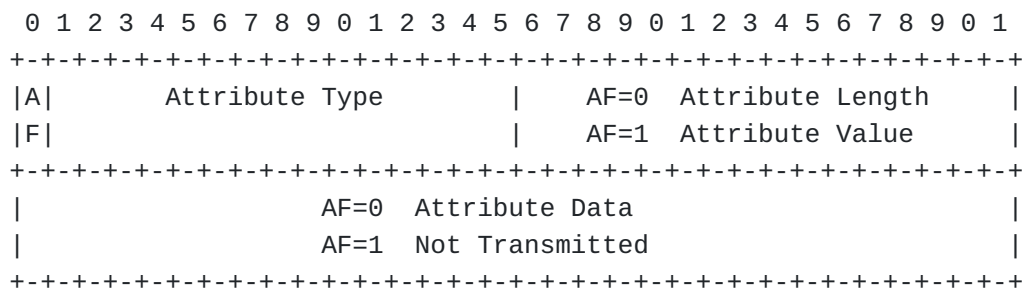


Figure 5: Transform Attribute Payload

For all parameter described in Figure 2, AF=1 and the Attribute Type constitutes the Parameter Code Point whose values are provided in Figure 6. When AF=1, The Attribute Value constitutes the Parameter Value and when AF=0, the Attribute Length constitutes the Parameter Value.

| Parameter Code Point | Designation | Reference |
|---|---|---|
| 0 | ehc_context_id | ThisRFC |
| 1 | alignment | ThisRFC |
| 2 | esp_spi_lsb | ThisRFC |
| 3 | esp_sn_lsb | ThisRFC |
| 4 | ts_flow_label | ThisRFC |
| 0 - 2 ** 15 - 1 | unallocated | |

Figure 6: Parameter Code Point Registry - The cod epoint is coded over 15 bits

For the ehc_context_id, the Parameter Value designates the EHC Context being negotiated. The description of such context must be defined. Currently only the Diet-ESP profile has been defined in [I-D.mglt-ipsecme-diet-esp].

| EHC Context Identifier Value | Designation | Reference | EHC Context Reference |
|---|---|---|---|
| 0 | Diet-ESP | ThisRFC | I-D.mglt-ipsecme-diet-esp |
| 1 - 2 ** 16 -1 | unallocated | | |

Figure 7: EHC Context Identifier

The alignment, esp_spi_lsb, esp_sn_lsb and ts_flow_label have a similar construction for there respective 16 bit Parameter Value. Each possible value is indicated by a bit. All other bits MUST be set to zero by the sender and MUST be ignored by the receiver. The initiator MAY set the a value is acceptable by setting the corresponding bit of that value. Multiple bits MAY be set. The responder MUST select a single bit.

For the alignment parameters, the first right most bit indicates an 32 bit alignment, the second right most bit indicates an 8 bit alignment.

For the esp_spi_lsb and esp_sn_lsb, the right most bit indicates a 4 byte LSB, the second right most bit indicates a 3 byte LSB, the third right most byte indicates a 2 byte LSB and the fourth right most bit indicates a 1 byte LSB.

For the alignment and the ts_flow_label parameters, the first right most bit indicates the value "True", the second right most bit indicates the value "False".

## 6. IANA section

This specification requests the IANA to create EHC Context Parameter Code Point registry ( see Figure 6) as well as a EHC Context Identifier registry (see Figure 7). Both registries are "Specification Required".

## 7. References

### 7.1. Normative References


**[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>.

**[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>.

### 7.2. Informative References

**[I-D.mglt-ipsecme-diet-esp]** Migault, D., Guggemos, T., Bormann, C., and D. Schinazi, "ESP Header Compression Profile", Work in Progress, Internet-Draft, draft-mglt-ipsecme-diet-esp-09, 28 June 2023, <https://datatracker.ietf.org/api/v1/doc/document/draft-mglt-ipsecme-diet-esp/>.

## Authors' Addresses

Daniel Migault
Ericsson

Email: daniel.migault@ericsson.com

Tobias Guggemos
LMU

Email: guggemos@nm.ifi.lmu.de

David Schinazi
Google LLC

Email: dschinazi.ietf@gmail.com