

ESP Header Compression Profile

`draft-mglt-ipsecme-diet-esp`

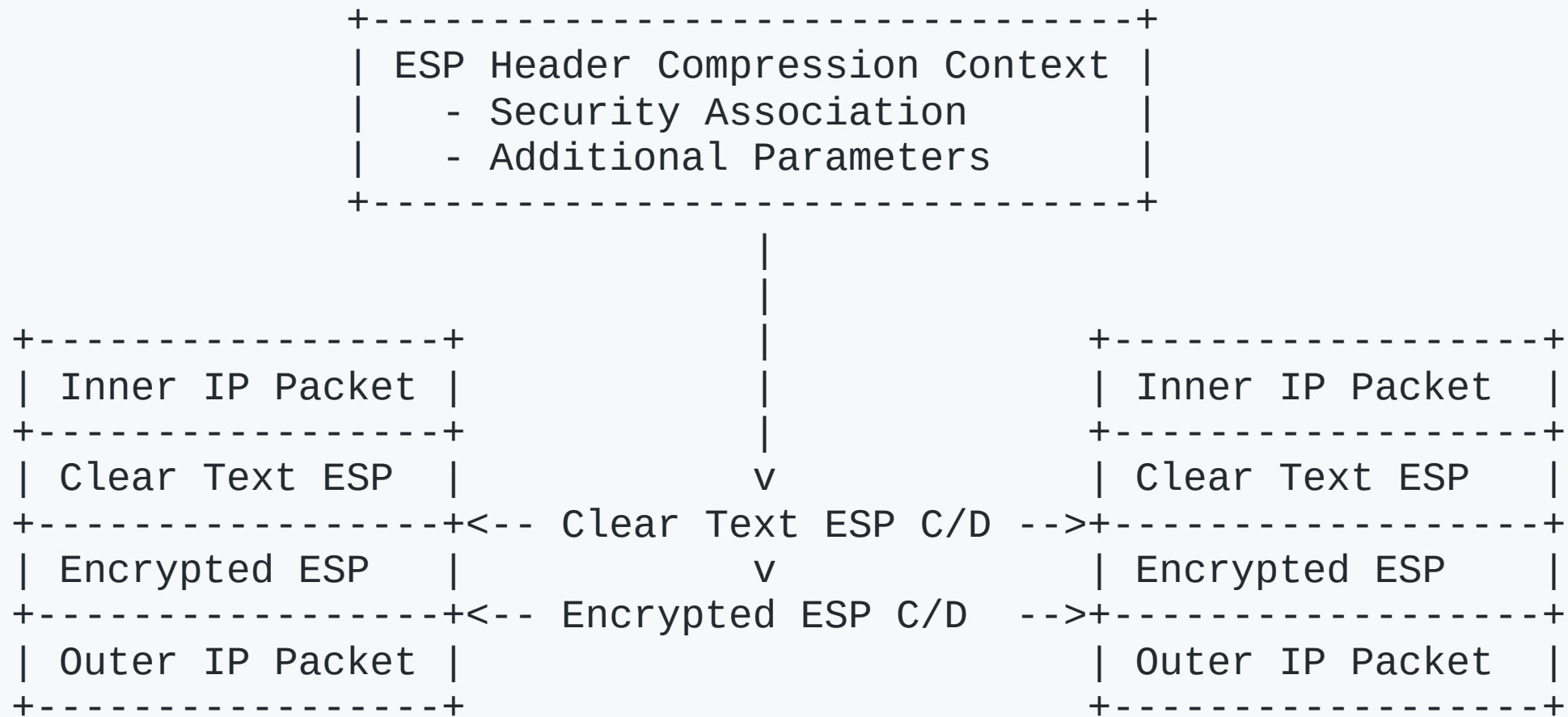
`draft-mglt-ipsecme-ikev2-diet-esp-extension`

Migault, Guggemos, Bormann, Schinazi

ESP Header Compression Profile (EHCP) defines a profile to compress communications protected with IPsec/ESP.

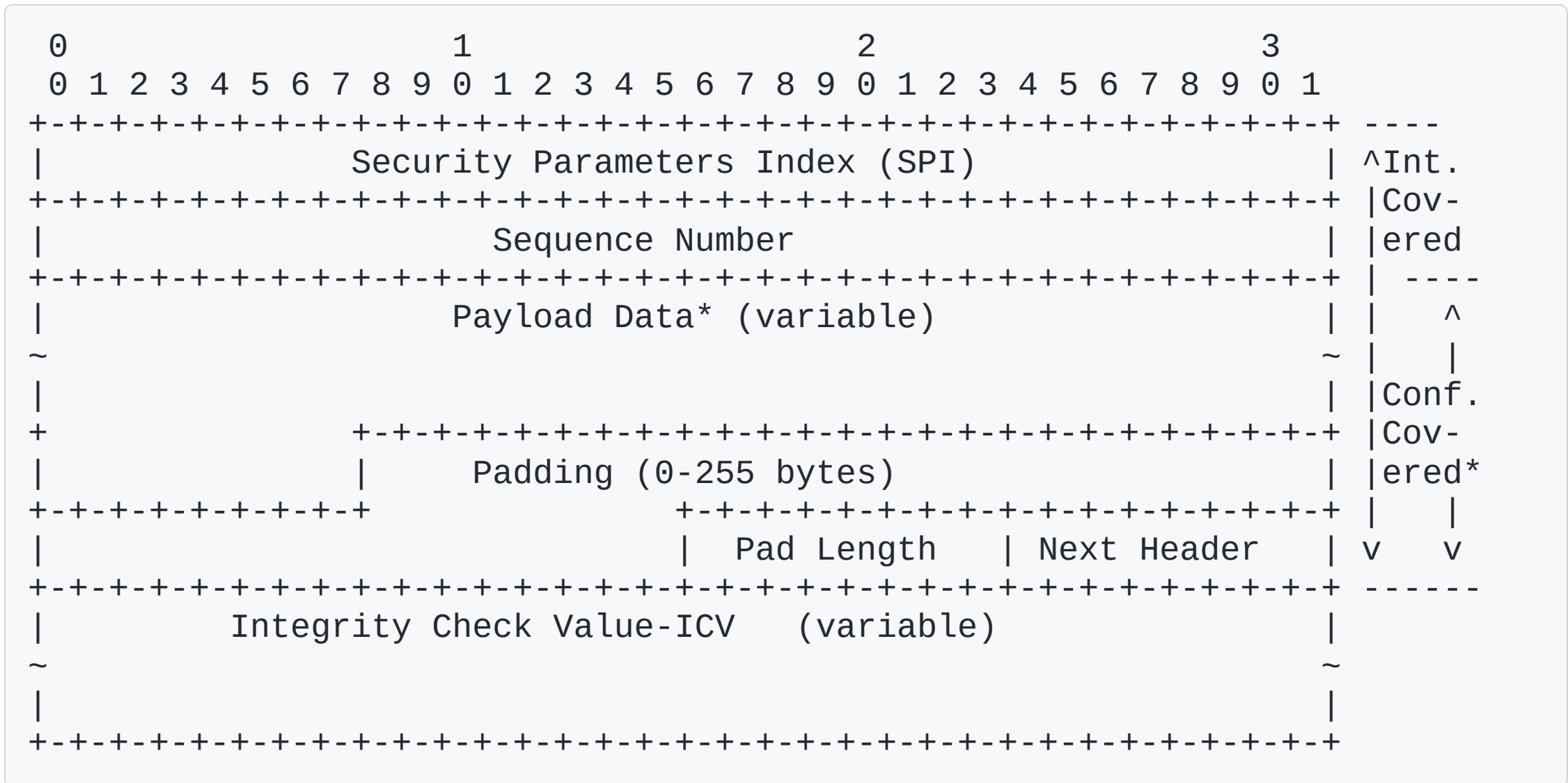
Compression / Decompression is based on the Generic Framework for Static Context Header (SCHC) [RFC8724].

- joint work with the SCHC WG



For a traditional VPN IPv6 in IPv6 we expect a 32 byte reduction.

Description of an ESP packet



EHC Context	Possible Values	Reference	C / D
alignment	"8 bit", "32 bit"	ThisRFC	CT E
ipsec_mode	"Tunnel", "Transport"	RFC4301	CT E
tunnel_ip	IPv4, IPv6 address	RFC4301	CT E
esp_spi	ESP SPI	RFC4301	EE
esp_spi_lsb	0, 1, 2, 3, 4*	ThisRFC	EE
esp_sn	ESP Sequence Number	RFC4301	EE
esp_sn_lsb	0, 1, 2, 3, 4*	ThisRFC	EE
esp_encr	ESP Encryption Algorithm	RFC4301	CT E
ts_flow_label	True, False	ThisRFC	CT E
ts_ip_version	4, 6	ThisRFC	CT E
ts_ip_src_start	IP4 or IPv6 address	ThisRFC	CT E
ts_ip_src_end	IP4 or IPv6 address	ThisRFC	CT E
ts_ip_dst_start	IPv4 or IPv6 address	ThisRFC	CT E
ts_ip_dst_end	IPv4 or IPv6 address	ThisRFC	CT E
ts_proto_list	TCP, UDP, ..., 0	ThisRFC	CT E
ts_port_src_start	Port number	ThisRFC	CT E
ts_port_src_end	Port number	ThisRFC	CT E
ts_port_dst_start	Port number	ThisRFC	CT E
ts_port_dst_end	Port number	ThisRFC	CT E
ts_dsp_list	DSCP number	RFCYYYY	CT E

The following parameters need to be agreed:

- alignment
- esp_spi_lsb
- esp_sn_lsb
- ts_flow_label

draft-mglt-ipsecme-ikev2-diet-esp-extension defines an IKEv2 extension EHC_SUPPORTED to agree on these parameters.

Where we are:

- We already implemented (contiki - without SCHC) Diet ESP:
 - [Diet-ESP: IP layer security for IoT](#) Journal of Computer Security, vol. 25, no. 2, pp. 173-203, 2017
- SCHC WG is integrating Diet-ESP in [openschc](#)

We believe the document is ready for adoption and we expect the implementation to be completed by the next IETF.

Thanks!

Initiator

Responder

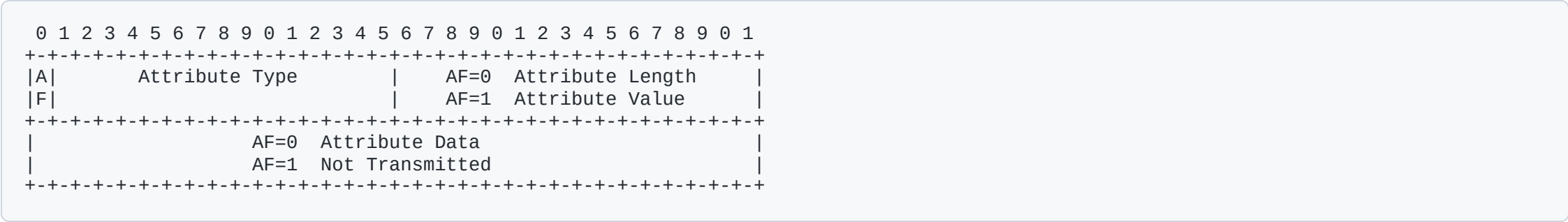
HDR, SA, KEi, Ni -->

<-- 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)

Parameters follow the same format as the Transform Attribute with AF=1



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	

EHC Context Identifier	Value	Designation	EHC Context Reference
0		Diet-ESP	draft-mglt-ipsecme-diet-esp
1 - 2 ** 16 - 1		unallocated	