

# Implicit IV for Counter-based Ciphers in IPsec

---

DRAFT-MGLT-IPSECME-IMPLICIT-IV

YOAV NIR – IETF 96 - BERLIN

# Why?

---

- Counter-based algorithms and AEADs are becoming more popular: AES-GCM, AES-CCM, ChaCha20.
- Unlike CBC-based algorithms, these do not benefit from unpredictable IVs. In fact, the specifications for all of these recommend using a guaranteed unique IV, specifically a counter as the recommended method of setting this IV.

# ESP Header

The diagram illustrates the structure of a 32-bit IPsec Security Association (SA) header. It is divided into four fields: SPI, Sequence Number, IV, and a large empty space. The SPI field is 16 bits long, containing the values 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1. The Sequence Number field is 16 bits long, containing the values 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1. The IV field is 16 bits long, containing the values 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1. The fourth field is 16 bits long and contains only vertical bars (|).

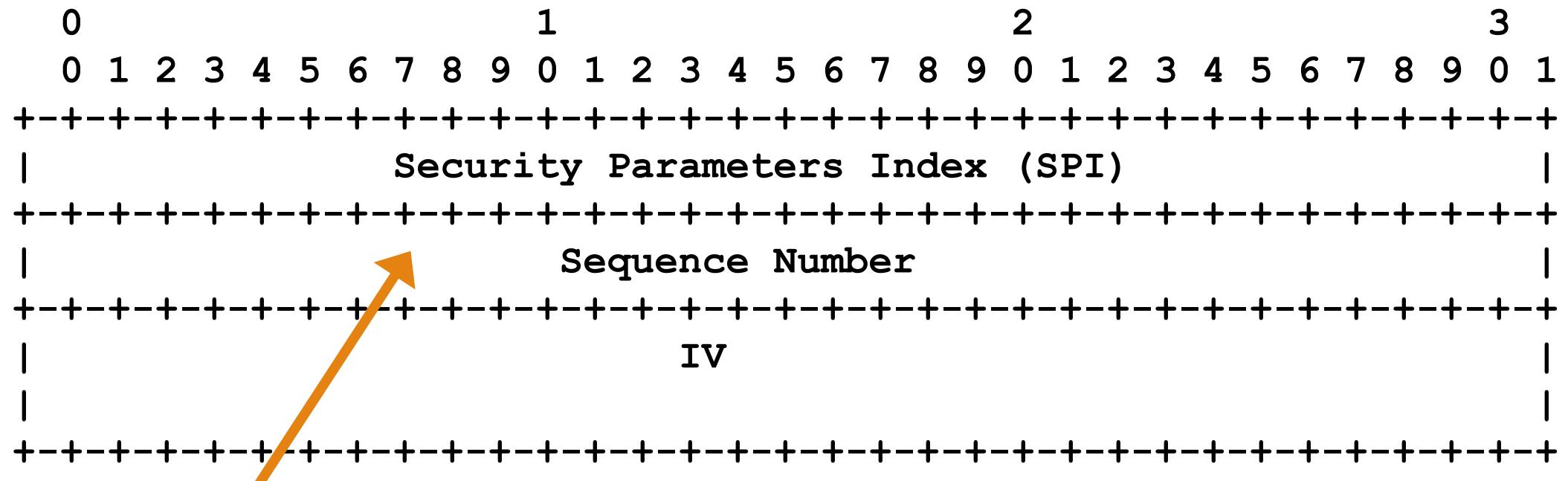
0	1	2	3
0	1	2	3
4	5	6	7
8	9	0	1
2	3	4	5
6	7	8	9
0	1	2	3
4	5	6	7
8	9	0	1
2	3	4	5
6	7	8	9
0	1	2	3

Security Parameters Index (SPI)

Sequence Number

IV

## ESP Header



This is a packet sequence number

# ESP Header

The diagram illustrates a 32-bit nonce structure. It is divided into four fields: SPI (Security Parameters Index), Sequence Number, and IV (Initialization Vector). The SPI field occupies the first 16 bits, the Sequence Number field occupies the next 8 bits, and the IV field occupies the final 8 bits. The IV field is highlighted with an orange arrow pointing to its first byte.

0	1	2	3												
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1	+	+	+												
Security Parameters Index (SPI)															
Sequence Number															
IV															
+	+	+	+												

# So is this

# Implicit IV

---

- If we follow the recommendations, those two counters will be equal.
- So why do we need to repeat the same counter in two different fields?
- We don't.
- If both sides agree, we can just omit the IV.
- It's optional anyway.
- Saves 8 bytes per packet.

# Negotiating Implicit IV

---

- Options:
  - New Transform Type
    - ENCR, INTEG, PFS, ESN, and now: IIV
  - New Transform Attribute
    - Key Length. Now also IIV
  - New Transform ID
    - Already have AES-GCM\_16; now also AES-GCM\_16\_IIV
  - New Notification

