

Network Working Group
Internet-Draft
Updates: 7296 (if approved)
Intended status: Standards Track
Expires: 17 September 2025

V. Smyslov
ELVIS-PLUS
16 March 2025

Renaming Extended Sequence Number (ESN) Transform Type in the Internet
Key Exchange Protocol Version 2 (IKEv2)
draft-ietf-ipsecme-ikev2-rename-esn-05

Abstract

This document clarifies and extends the meaning of transform type 5 in IKEv2. It updates RFC 7296 by renaming the transform type 5 from "Extended Sequence Numbers (ESN)" to "Sequence Numbers (SN)". It also renames two currently defined values for this transform type: value 0 from "No Extended Sequence Numbers" to "32-bit Sequential Numbers" and value 1 from "Extended Sequence Numbers" to "Partially Transmitted 64-bit Sequential Numbers".

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.

Copyright Notice

Copyright (c) 2025 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 (<https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Problem Description	3
3. Extending the Semantics of Transform Type 5	4
4. Security Considerations	6
5. IANA Considerations	6
6. Acknowledgements	7
7. References	7
7.1. Normative References	7
7.2. Informative References	8
Author's Address	9

1. Introduction

IP Security (IPsec) Architecture [RFC4301] defines a set of security services provided by IPsec protocols Authentication Header (AH) [RFC4302] and Encapsulating Security Payload (ESP) [RFC4303]. One of these services is replay protection, which is referred to as "anti-replay" in these documents. In IPsec the anti-replay service is optional, each receiver of AH and/or ESP packets can choose whether to enable it on a per Security Association (SA) basis. The replay protection in AH and ESP is achieved by means of a monotonically increasing counter that never wraps around, which is sent in each AH or ESP packet in the Sequence Number field. The receiver maintains a sliding window that allows to detect duplicate packets.

Both AH and ESP allow using either a 32-bit counter or a 64-bit counter. The latter case is referred to as Extended Sequence Numbers (ESN) in AH and ESP specifications. Since the Sequence Number field in both AH and ESP headers is only 32 bits in size, in case of ESN the high-order 32 bits of the counter are not transmitted and are determined by the receiver based on previously received packets.

Since the decision whether to enable the anti-replay service is taken by the receiver based only on the receiver's local policy, the sender in accordance with the specifications for AH ([RFC4302] Section 3.3.2) and ESP ([RFC4303] Section 3.3.3) should always assume that the replay protection is enabled on receiving side. Thus, the sender should always send the increasing counter values and should take care that the counter never wraps around. AH and ESP specifications also discuss situations when replay protection is not possible to achieve even if senders do all as prescribed -- like in multicast Security Associations with multiple unsynchronized senders.

Both AH and ESP specifications allow the sender to avoid maintaining the counter if the sender has been notified somehow that the anti-replay service is disabled by the receiver or is not possible to achieve.

AH and ESP Security Associations are usually established using the Internet Key Exchange protocol version 2 (IKEv2) [RFC7296]. The process of SA establishment includes calculation of a shared key and negotiation of various SA parameters, such as cryptographic algorithms. This negotiation in IKEv2 is performed via transforms (see Section 3.3.2 of [RFC7296]). The type of transform determines what parameter is being negotiated. Each transform type has an associated list of possible values (called Transform IDs), that determine the possible options for negotiation. See [IKEV2-IANA] for the list of transform types and associated transform IDs.

Transform type 5 "Extended Sequence Numbers (ESN)" is used in IKEv2 to negotiate the way sequence numbers for replay protection are generated, transmitted and processed in the context of an SA. For this transform type two values are defined -- "No Extended Sequence Numbers" and "Extended Sequence Numbers".

This document updates IKEv2 specification [RFC7296] by renaming transform type 5 and two associated transform IDs.

2. Problem Description

IKEv2 currently has no means to negotiate the case when both peers agree that replay protection is not needed. Even when both peers locally disable anti-replay service as receivers, they still need to maintain increasing sequence numbers as senders, taking care that they never wrap around (see [I-D.pan-ipsecme-anti-replay-notification]).

There is also no way to inform receivers that replay protection is not possible for a particular SA (for example in case of a multicast SA with several unsynchronized senders).

Future IPsec security protocols may provide more options for the handling of anti-replay counters, like sending full 64-bit sequence numbers or completely omitting them in packets (see [I-D.klassert-ipsecme-eesp]). These options will require means to be negotiated in IKEv2.

Transform type 5 is the best candidate for addressing these issues: it is already used for negotiation of how sequence numbers are handled in AH and ESP and it is possible to define additional transform IDs that could be used in the corresponding situations.

However, the current definition of transform type 5 is too narrow -- its name implies that this transform can only be used for negotiation of using ESN.

3. Extending the Semantics of Transform Type 5

This document extends the semantics of transform type 5 in IKEv2 to the following definition.

Transform type 5 defines the set of properties of sequence numbers of IPsec packets of a given SA when these packets enter the network.

This definition requires some clarifications.

- * By "sequence numbers" here we assume logical entities (like counters) that can be used for replay protection on receiving sides. In particular, these entities are not necessarily the content of the Sequence Number field in the IPsec packets, but may be constructed using some information, that is not necessarily transmitted.
- * The properties are interpreted as a characteristic of IPsec SA packets, and not as a result of a sender actions. For example, in multicast SA with multiple unsynchronized senders, even if each sender ensures the uniqueness of sequence numbers it generates, the uniqueness of sequence numbers for all IPsec packets is not guaranteed.
- * The properties are defined for the packets just entering the network and not for the packets that receivers get. This is because network behavior may break some of these properties (e.g., break sequence numbers uniqueness by packet duplication).
- * The properties of sequence numbers are interpreted in a broad sense, that includes the case when sequence numbers are absent.

Given this definition, transform type 5 in the IANA registries for IKEv2 [IKEV2-IANA] is renamed from "Extended Sequence Numbers (ESN)" to "Sequence Numbers (SN)" with the meaning, that it defines the properties the sequence numbers would have.

It is expected that new transform IDs will be defined for this transform type in future (like in G-IKEv2 [I-D.ietf-ipsecme-g-ikev2] for the case of multicast SAs). Documents defining new transform IDs should include description of the properties the sequence numbers would have if the new transform ID is selected. In particular, this description should include discussion whether these properties allow achieving replay protection.

Some existing protocols (like Implicit IV in ESP [RFC8750] or Aggregation and Fragmentation for ESP [RFC9347]) rely on properties that are guaranteed for the currently defined transform IDs, but this might not be true for future transform IDs. When a new transform ID is defined, its description should include a discussion about the possibility of using this transform ID in protocols, that rely on some particular properties of sequence numbers.

The two currently defined transform IDs for this transform type define the following properties of sequence numbers.

- * Value 0 for transform type 5 defines sequence numbers as monotonically increasing 32-bit counters that are transmitted in the Sequence Number field of AH and ESP packets. They never wrap around and are guaranteed to be unique, thus they are suitable for replay protection. They can also be used with protocols that rely on sequence numbers uniqueness (like [RFC8750]) or their monotonic increase (like [RFC9347]). The sender and the receiver actions are defined in Sections 3.3.2 and 3.4.3 of [RFC4302] for AH and in Sections 3.3.3 and 3.4.3 of [RFC4303] for ESP.
- * Value 1 for transform type 5 defines sequence numbers as monotonically increasing 64-bit counters. The low-order 32 bits are transmitted in the Sequence Number field of AH and ESP packets and the high-order 32 bits are implicitly determined on receivers based on previously received packets. The sequence numbers never wrap around and are guaranteed to be unique, thus they are suitable for replay protection. They can also be used with protocols that rely on sequence numbers uniqueness (like [RFC8750]) or their monotonic increase (like [RFC9347]). To be able to correctly process the incoming packets on receivers the packets must be authenticated (even when the replay protection is not used). The sender and the receiver actions are defined in Sections 3.3.2 and 3.4.3 of [RFC4302] for AH and in Sections 3.3.3 and 3.4.3 of [RFC4303] for ESP.

Given the descriptions above and the new definition of transform type 5, the two currently defined transform IDs are renamed to better reflect the properties of sequence numbers they assume.

- * Transform ID 0 is renamed from "No Extended Sequence Numbers" to "32-bit Sequential Numbers".
- * Transform ID 1 is renamed from "Extended Sequence Numbers" to "Partially Transmitted 64-bit Sequential Numbers".

Note, that the above descriptions do not change the existing semantics of these transform IDs, they only provide clarification. Note also, that ESP and AH packet processing for these transform IDs is not affected, and bits on the wire do not change.

4. Security Considerations

This document does not affect security of the AH, ESP and IKEv2 protocols.

5. IANA Considerations

This document makes the following changes in the "Internet Key Exchange Version 2 (IKEv2) Parameters" IANA registries [IKEV2-IANA]. It is assumed that RFCXXXX refers to this specification.

- * The existing transform type 5 "Extended Sequence Numbers (ESN)" in the "Transform Type Values" registry is renamed to "Sequence Numbers (SN)".
- * Appended [RFCXXXX] to the Reference column of Transform Type 5 in the "Transform Type Values" registry.
- * Added this note to the "Transform Type Values" registry:

"Sequence Numbers (SN)" transform type was originally named "Extended Sequence Numbers (ESN)" and was referenced by that name in a number of RFCs published prior to [RFCXXXX], which gave it the current title.
- * The "Transform Type 5 - Extended Sequence Numbers Transform IDs" registry is renamed to "Transform Type 5 - Sequence Numbers Transform IDs".
- * The "Reserved" (2-65535) range of numbers in what was the "Transform Type 5 - Extended Sequence Numbers Transform IDs" registry is split into the "Unassigned" (2-1023) and the "Reserved for Private Use" (1024-65535) ranges, as shown below.

Number	Name	Reference

2-1023	Unassigned	
1024-65535	Reserved for Private Use	[RFCXXXX]

- * The existing Transform ID 0 "No Extended Sequence Numbers" in what was the "Transform Type 5 - Extended Sequence Numbers Transform IDs" registry is renamed to "32-bit Sequential Numbers".

- * The existing Transform ID 1 "Extended Sequence Numbers" in what was the "Transform Type 5 - Extended Sequence Numbers Transform IDs" registry is renamed to "Partially Transmitted 64-bit Sequential Numbers".
- * Appended [RFCXXXX] to the Reference column of Transform ID 0 and Transform ID 1 in what was the "Transform Type 5 - Extended Sequence Numbers Transform IDs" registry.
- * Added these notes to what was the "Transform Type 5 - Extended Sequence Numbers Transform IDs" registry:

This registry was originally named "Transform Type 5 - Extended Sequence Numbers Transform IDs" and was referenced using that name in a number of RFCs published prior to [RFCXXXX], which gave it the current title.

"32-bit Sequential Numbers" transform ID was originally named "No Extended Sequence Numbers" and was referenced by that name in a number of RFCs published prior to [RFCXXXX], which gave it the current title.

"Partially Transmitted 64-bit Sequential Numbers" transform ID was originally named "Extended Sequence Numbers" and was referenced by that name in a number of RFCs published prior to [RFCXXXX], which gave it the current title.

Numbers in the range 2-65535 were originally marked as "Reserved" and were re-classified as "Unassigned" and "Reserved for Private Use" by [RFCXXXX].

6. Acknowledgements

This document was created as a result of discussions with Russ Housley, Tero Kivinen, Paul Wouters and Antony Antony about the best way to extend the meaning of the Extended Sequence Numbers transform in IKEv2.

7. References

7.1. Normative References

[IKEV2-IANA]

IANA, "Internet Key Exchange Version 2 (IKEv2) Parameters", <<http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml>>.

- [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>>.
- [RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <<https://www.rfc-editor.org/info/rfc4302>>.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <<https://www.rfc-editor.org/info/rfc4303>>.
- [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>>.

7.2. Informative References

- [I-D.ietf-ipsecme-g-ikev2]
Smyslov, V. and B. Weis, "Group Key Management using IKEv2", Work in Progress, Internet-Draft, draft-ietf-ipsecme-g-ikev2-21, 10 February 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-g-ikev2-21>>.
- [I-D.klassert-ipsecme-eesp]
Klassert, S., Antony, A., and C. Hopps, "Enhanced Encapsulating Security Payload (EESP)", Work in Progress, Internet-Draft, draft-klassert-ipsecme-eesp-02, 26 February 2025, <<https://datatracker.ietf.org/doc/html/draft-klassert-ipsecme-eesp-02>>.
- [I-D.pan-ipsecme-anti-replay-notification]
Pan, W., He, Q., and P. Wouters, "IKEv2 Support for Anti-Replay Status Notification", Work in Progress, Internet-Draft, draft-pan-ipsecme-anti-replay-notification-01, 21 October 2024, <<https://datatracker.ietf.org/doc/html/draft-pan-ipsecme-anti-replay-notification-01>>.
- [RFC8750] Migault, D., Guggemos, T., and Y. Nir, "Implicit Initialization Vector (IV) for Counter-Based Ciphers in Encapsulating Security Payload (ESP)", RFC 8750, DOI 10.17487/RFC8750, March 2020, <<https://www.rfc-editor.org/info/rfc8750>>.

[RFC9347] Hopps, C., "Aggregation and Fragmentation Mode for Encapsulating Security Payload (ESP) and Its Use for IP Traffic Flow Security (IP-TFS)", RFC 9347, DOI 10.17487/RFC9347, January 2023, <<https://www.rfc-editor.org/info/rfc9347>>.

Author's Address

Valery Smyslov
ELVIS-PLUS
Russian Federation
Email: svan@elvis.ru