Internet Engineering Task Force (IETF)
Request for Comments: 9827
Updates: 7296
Category: Standards Track
ISSN: 2070-1721

V. Smyslov
ELVIS-PLUS

November 2025

Renaming the Extended Sequence Numbers (ESN) Transform Type in the Internet Key Exchange Protocol Version 2 (IKEv2)

Abstract

This document clarifies and extends the meaning of Transform Type 5 in Internet Key Exchange Protocol Version 2 (IKEv2). It updates RFC 7296 by renaming 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9827.

Table of Contents

1. Introduction

The IP Security (IPsec) Architecture [RFC4301] defines a set of security services provided by the 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 and is sent in each AH or ESP packet in the Sequence Number field. The receiver maintains a sliding window that allows duplicate packets to be detected.

Both AH and ESP allow use of 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.

The receiver decides whether to enable the anti-replay service based only on the receiver’s local policy, so 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 the 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 in which 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 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 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. There are two values are defined for this Transform Type -- "No Extended Sequence Numbers" and "Extended Sequence Numbers".

This document updates the IKEv2 specification [RFC7296] by renaming Transform Type 5 and the 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 [ANTIREPLAY]).

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 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 [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 be defined as follows:

> 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 updated definition is clarified as follows:

* "Sequence numbers" in this definition are not necessarily the content of the Sequence Number field in the IPsec packets; they may also be some logical entities (e.g., counters) that could be constructed taking some information that is not transmitted on the wire into account.

* The properties are interpreted as characteristics of IPsec SA packets rather than the results of 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., packet duplication would break sequence number uniqueness).

* The properties of sequence numbers are interpreted in a broad sense, which includes the case when sequence numbers are absent.

Given this updated definition, Transform Type 5 in the "Transform Type Values" registry [IKEV2-IANA] has been renamed from "Extended Sequence Numbers (ESN)" to "Sequence Numbers (SN)" in the sense that it defines the properties of the sequence numbers in general.

It is expected that new Transform IDs will be defined for this Transform Type in the future (like in G-IKEv2 [RFC9838] for the case of multicast SAs). Documents defining new Transform IDs should include descriptions of the properties the sequence numbers would have if the new Transform ID was selected. In particular, the descriptions should include discussion of whether these properties allow replay protection to be achieved.

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; however, this might not be true for future Transform IDs. When a new Transform ID is defined, its description should include discussion about the possibility of using the Transform ID in protocols that rely on some particular properties of sequence numbers.

The two currently defined Transform IDs for Transform Type 5 define the following properties of sequence numbers.

* Value 0 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 number uniqueness (e.g., [RFC8750]) or monotonically increasing sequence numbers (e.g., [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 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 number uniqueness (e.g., [RFC8750]) or their monotonic increase (e.g., [RFC9347]). 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. Also note 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 changes to registries within the "Internet Key Exchange Version 2 (IKEv2) Parameters" registry group [IKEV2-IANA].

The "Transform Type Values" registry has been updated as follows:

* renamed Transform Type 5 from "Extended Sequence Numbers (ESN)" to "Sequence Numbers (SN)".

* added as a reference to this RFC for Transform Type 5.

* added the following note:

  | The "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 [RFC9827], which
  | gave it the current title.

The "Transform Type 5 - Extended Sequence Numbers Transform IDs" registry has been updated as follows:

* renamed the registry from "Transform Type 5 - Extended Sequence Numbers Transform IDs" to "Transform Type 5 - Sequence Numbers Transform IDs" and added this document as a reference.

* split the "Reserved" (2-65535) range of numbers as shown below.

Number	Name	Reference
2-1023	Unassigned	
1024-65535	Reserved for Private Use	[RFC9827]

Table 1

* renamed Transform ID 0 from "No Extended Sequence Numbers" to "32-bit Sequential Numbers".

* renamed Transform ID 1 from "Extended Sequence Numbers" to "Partially Transmitted 64-bit Sequential Numbers".

* added a reference to this RFC for Transform ID 0 and Transform ID 1.

* added the following registry notes:

  | 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 [RFC9827], which gave it the current title.

  | The "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 [RFC9827], which gave it the current title.

  | The "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 [RFC9827], which gave it the current title.

  | Numbers in the range 2-65535 were originally marked as "Reserved" and were reclassified as "Unassigned" and "Reserved for Private Use" by [RFC9827].

6. References

6.1. Normative References

[IKEV2-IANA] IANA, "Internet Key Exchange Version 2 (IKEv2) Parameters", <http://www.iana.org/assignments/ikev2-parameters>.

[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>.

6.2. Informative References

[ANTIREPLAY] 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>.

[EESP] Klassert, S., Antony, A., and C. Hopps, "Enhanced Encapsulating Security Payload (EESP)", Work in Progress, Internet-Draft, draft-ietf-ipsecme-eesp-02, 19 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-eesp-02>.

[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>.

[RFC9838] Smyslov, V. and B. Weis, "Group Key Management Using the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9838, DOI 10.17487/RFC9838, November 2025, <https://www.rfc-editor.org/info/rfc9838>.

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.

Author’s Address

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