IPsecME
Internet-Draft
Intended status: Experimental
Expires: 2 October 2025

Y. Sakemi
S. Kanno
GMO Cybersecurity by Ierae, Inc.

31 March 2025

The Areion Cipher Algorithm and Its Use With IPsec
draft-sakemi-ipsec-areion-00

Abstract

This document specifies the integration of the Areion cryptographic permutation into IPsec. Areion is a novel cryptographic primitive designed to achieve significantly lower latency for encryption and hashing operations compared to traditional algorithms like AES-GCM, making it particularly suitable for high-performance VPNs and data center interconnect scenarios. This specification defines the use of Areion within Encapsulating Security Payload (ESP), including the associated keying materials and the necessary parameters for Internet Key Exchange (IKE).

The Areion permutation is fully described in [I-D.sakemi-areion]. This document focuses on incorporating Areion into IPsec.

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 2 October 2025.

Table of Contents

1. Introduction

IPsec RFC4301 [RFC4303] provides mechanisms to ensure confidentiality, integrity, and authenticity of IP datagrams. A key component of IPsec is the choice of cryptographic permutations that can meet the performance and security requirements of diverse environments. Traditional algorithms such as AES-GCM [RFC4106] are widely deployed due to their proven track record, and general AEAD guidelines are provided in [RFC5116]. However, as network speeds increase and latency-sensitive applications proliferate, there is a growing need for cryptographic permutations optimized for low latency.

The Areion [I-D.sakemi-areion] is designed as a low-latency cryptographic permutation, offering both confidentiality and integrity within a single primitive. By leveraging Areion within IPsec ESP and negotiating its parameters via IKE [RFC7296], we can achieve efficient, scalable, and interoperable secure communications.

2. Conventions and Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT","SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC8174].

3. Overview of Areion permutation in IPsec

Areion [I-D.sakemi-areion] aims to reduce latency by integrating both encryption and hashing into a single permutation. This integration eliminates the overhead of separate operations, making it suitable for high-speed networks and latency-critical environments.

4. IPsec Integration

4.1. Keying Material

Areion uses a single session key from which sub-keys are derived for encryption and hashing. These keys are negotiated and derived through the IKE protocol [RFC7296], in accordance with the procedures defined in [I-D.sakemi-areion].

4.2. ESP Processing

When used with ESP [RFC4303], Areion replaces the conventional encryption and integrity algorithms:

1. *Encryption*: ESP payloads are encrypted block-by-block using Areion.

2. *Integrity*: The integrated hashing function simultaneously computes an authentication tag appended to the packet.

3. *Nonce Handling*: A per-packet nonce is used as described in [I-D.sakemi-areion].

The ESP header format remains unchanged, and the SPI, sequence number, and other fields operate as defined in [RFC4303].

5. IKE Negotiation

Support for Areion is negotiated via IKE [RFC7296]. The IKE initiator and responder include the Areion permutation in their proposals, and if both agree, Areion is used for ESP encryption and integrity. Parameters such as key size and tag length are defined in [I-D.sakemi-areion]. Implementations MUST support the key sizes and tag lengths specified in the Areion document.

6. Security Considerations

The security considerations described in [I-D.sakemi-areion] apply. Areion aims to provide security properties comparable to widely deployed algorithms like AES-GCM [RFC4106]. Implementers must ensure proper key management, nonce usage (as detailed in [I-D.sakemi-areion]), and compliance with IPsec replay protection rules as defined in [RFC4301]. Special attention SHOULD be paid to the generation of unique nonces for each packet to prevent replay attacks when using Areion with ESP.

7. IANA Considerations

For negotiating use of Areion for encryption algorithm, IANA is requested to assign two Transform IDs to the "Transform Type 1 - Encryption Algorithm Transform IDs" registry:

Number	Name	ESP Reference	IKEv2 Reference
TBD	ENCR_AREION_OPP	[This draft]	[This draft]
TBD	ENCR_AREION_OTR	[This draft]	[This draft]

Table 1: Areion Transform IDs

For negotiating use of Areion as PRFs for IKEv2, IANA is requested to assign a new Transform IDs in the "Transform Type 2 - Pseudorandom Function Transform IDs" registry:

Number	Name	Status	Reference	
	TBD	PRF_HMAC_AREION_256		[This draft]

Table 2: Areion PRF Transform IDs

For negotiating use of Areion for integrity protection in IKEv2 and IPsec protocols, IANA is requested to assign a new Transform IDs in the "Transform Type 3 - Integrity Algorithm Transform IDs" registry:

Number	Name	Status	Reference
TBD	AUTH_HMAC_AREION_256_128		[This draft]

Table 3: Areion Integrity Algorithm Transform IDs

8. References

8.1. Normative References

[I-D.sakemi-areion]
Sakemi, Y. and S. Kanno, "Ultra-Low Latency Cryptography Areion", Work in Progress, Internet-Draft, draft-sakemi-areion-00, 23 October 2023, <https://datatracker.ietf.org/doc/html/draft-sakemi-areion-00>.

[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/rfc/rfc2119>.

[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/rfc/rfc4301>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/rfc8174>.

8.2. Informative References

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, DOI 10.17487/RFC4106, June 2005, <https://www.rfc-editor.org/rfc/rfc4106>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <https://www.rfc-editor.org/rfc/rfc5116>.

Appendix A. Test Vectors

Test vectors for the Areion cryptographic permutation in IPsec are provided below to assist implementers with verification and interoperability testing. Actual test vectors including keys, nonces, plaintext, ciphertext, and authentication tags are TBD and will be specified in future revisions of this document.

Authors' Addresses

Yumi Sakemi
GMO Cybersecurity by Ierae, Inc.
Email: yumi.sakemi@gmo-cybersecurity.com

Satoru Kanno
GMO Cybersecurity by Ierae, Inc.
Email: satoru.kanno@gmo-cybersecurity.com