(No Working Group)
Internet-Draft
Intended status: Informational
Expires: May 11, 2019

G. Amringer
Independent

November 7, 2018

Chacha derived AEAD algorithms in JSON Object Signing and Encryption (JOSE)
draft-amringer-jose-chacha-00

Abstract

This document defines how to use the AEAD algorithms "AEAD_XCHACHA20_POLY1305" and "AEAD_CHACHA20_POLY1305" from [RFC8439] and [I-D.arciszewski-xchacha] in JSON Object Signing and Encryption (JOSE).

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 May 11, 2019.

Table of Contents

1. Introduction

The Internet Research Task Force (IRTF) Crypto Forum Research Group (CFRG) defined the ChaCha20 and Poly1305 algorithms to be used in IETF protocols both independantly and as an AEAD construction ([RFC8439]). It has also been presented with a definition of an eXtended-nonce variant ([I-D.arciszewski-xchacha]) for use in stateless contexts. This document defines how to use those algorithms in JOSE in an interoperable manner.

This document defines the conventions to use in the context of [RFC7516], and [RFC7517].

1.1. Notation and Conventions

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].

The JOSE key format ("JSON Web Key (JWK)") is defined by [RFC7517] and thumbprints for it ("JSON Web Key (JWK) Thumbprint") in [RFC7638].

2. Key Management

2.1. Algorithms

This section defines the specifics of encrypting a JWE Content Encryption Key (CEK) with AEAD_CHACHA20_POLY1305 ([RFC8439]) and AEAD_XCHACHA20_POLY1305 ([I-D.arciszewski-xchacha]).

Use of an Initialization Vector (IV) is REQUIRED with this algorithm. The IV is represented in base64url-encoded form as the "iv" (initialization vector) Header Parameter value.

The Additional Authenticated Data value used is the empty octet string.

The JWE Encrypted Key value is the ciphertext output.

The Authentication Tag output is represented in base64url-encoded form as the "tag" (authentication tag) Header Parameter value.

The following "alg" (algorithm) Header Parameter values are used to indicate that the JWE Encrypted Key is the result of encrypting the CEK using the corresponding algorithm and IV size:

Algorithm	IV size	"alg" value
AEAD_CHACHA20_POLY1305	96 bits	C20PKW
AEAD_XCHACHA20_POLY1305	192 bits	XC20PKW

2.2. Header Parameters Used for Key Encryption

The following Header Parameters are used for both algorithms defined for key encryption.

2.2.1. "iv" (Initialization Vector) Header Parameter

The "iv" (initialization vector) Header Parameter value is the base64url-encoded representation of the 96-bit or 192-bit IV value used for the key encryption operation. This Header Parameter MUST be present and MUST be understood and processed by implementations when these algorithms are used.

2.2.2. "tag" (Authentication Tag) Header Parameter

The "tag" (authentication tag) Header Parameter value is the base64url-encoded representation of the 128-bit Authentication Tag value resulting from the key encryption operation. This Header Parameter MUST be present and MUST be understood and processed by implementations when these algorithms are used.

3. Content Encryption

3.1. Algorithms

This section defines the specifics of performing authenticated encryption with ChaCha20-Poly1305.

The CEK is used as the encryption key.

Use of an IV is REQUIRED with this algorithm.

The following "enc" (encryption algorithm) Header Parameter values are used to indicate that the JWE Ciphertext and JWE Authentication Tag values have been computed using the corresponding algorithm and IV size:

Algorithm	IV size	"alg" value
AEAD_CHACHA20_POLY1305	96 bits	C20P
AEAD_XCHACHA20_POLY1305	192 bits	XC20P

4. IANA Considerations

The following is added to the "JSON Web Signature and Encryption Algorithms" registry:

- Algorithm Name: "C20PKW"
- Algorithm Description: Key wrapping with ChaCha20-Poly1305
- Algorithm Usage Location(s): "alg"
- JOSE Implementation Requirements: Recommended
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC-THIS]
- Algorithm Analysis Documents(s): [RFC8439]

- Algorithm Name: "XC20PKW"
- Algorithm Description: Key wrapping with XChaCha20-Poly1305
- Algorithm Usage Location(s): "alg"
- JOSE Implementation Requirements: Recommended
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC-THIS]
- Algorithm Analysis Documents(s): [I-D.arciszewski-xchacha]

- Algorithm Name: "C20P"
- Algorithm Description: ChaCha20-Poly1305
- Algorithm Usage Location(s): "enc"
- JOSE Implementation Requirements: Recommended

- o Change Controller: IESG
- o Specification Document(s): Section 3 of [RFC-THIS]
- o Algorithm Analysis Documents(s): [RFC8439]

- o Algorithm Name: "XC20P"
- o Algorithm Description: ChaCha20-Poly1305
- o Algorithm Usage Location(s): "enc"
- o JOSE Implementation Requirements: Recommended
- o Change Controller: IESG
- o Specification Document(s): Section 3 of [RFC-THIS]
- o Algorithm Analysis Documents(s): [I-D.arciszewski-xchacha]

5. Normative References

[I-D.arciszewski-xchacha]
Arciszewski, S., "XChaCha: eXtended-nonce ChaCha and AEAD_XChaCha20_Poly1305", draft-arciszewski-xchacha-02 (work in progress), October 2018.

[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/info/rfc2119>.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, <https://www.rfc-editor.org/info/rfc7516>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/info/rfc7517>.

[RFC7638] Jones, M. and N. Sakimura, "JSON Web Key (JWK) Thumbprint", RFC 7638, DOI 10.17487/RFC7638, September 2015, <https://www.rfc-editor.org/info/rfc7638>.

[RFC8439] Nir, Y. and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols", RFC 8439, DOI 10.17487/RFC8439, June 2018, <https://www.rfc-editor.org/info/rfc8439>.

Author's Address

Guillaume Amringer
Independent
Canada

Email: g.amringer@gmail.com