JOSE Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 15, 2014

M. Jones
Microsoft

July 14, 2013

Key Wrapping with AES GCM for JWE
draft-jones-jose-aes-gcm-key-wrap-01

Abstract

This specification defines how to encrypt (wrap) keys with the AES GCM algorithm for JSON Web Encryption (JWE) objects.

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 http://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 January 15, 2014.

Copyright Notice

Table of Contents

1. Introduction

This specification defines how to encrypt (wrap) keys with the AES GCM algorithm [AES] [NIST.800-38D] for JSON Web Encryption (JWE) [JWE] objects.

1.1. Notational 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 Key words for use in RFCs to Indicate Requirement Levels [RFC2119].

2. Terminology

This specification uses the same terminology as the JSON Web Encryption (JWE) [JWE] and JSON Web Algorithms (JWA) [JWA] specifications.

3. Key Encryption with AES GCM

This section defines the specifics of encrypting a JWE Content Encryption Key (CEK) with Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) [AES] [NIST.800-38D] using 128 or 256 bit keys. The "alg" header parameter values "A128GCMKW" or "A256GCMKW" are respectively used in this case.

Use of an Initialization Vector of size 96 bits is REQUIRED with this algorithm. The Initialization Vector 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 requested size of the Authentication Tag output MUST be 128 bits, regardless of the key size.

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.

3.1. Header Parameters Used for AES GCM Key Encryption

The following Header Parameter Names are used for AES GCM key encryption. They MAY also be used by other algorithms if so specified by those algorithm parameter definitions.

3.1.1. "iv" (Initialization Vector) Header Parameter

The "iv" (initialization vector) header parameter value is the base64url encoded representation of the Initialization Vector value used for the key encryption operation. This Header Parameter is REQUIRED and MUST be understood and processed by implementations when these algorithms are used.

3.1.2. "tag" (Authentication Tag) Header Parameter

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

4. IANA Considerations

4.1. JSON Web Signature and Encryption Algorithms Registration

This specification registers the algorithms defined in Section 3 in the JSON Web Signature and Encryption Algorithms registry [JWA].

4.1.1. Registry Contents

- Algorithm Name: "A128GCMKW"
- Algorithm Usage Location(s): "alg"
- Implementation Requirements: OPTIONAL
- Change Controller: IETF
- Specification Document(s): Section 3 of [[this document]]

- Algorithm Name: "A256GCMKW"
- Algorithm Usage Location(s): "alg"
- Implementation Requirements: OPTIONAL
- Change Controller: IETF
- Specification Document(s): Section 3 of [[this document]]

4.2. Registration of JWE Header Parameter Names

This specification registers the Header Parameter Names defined in Section 3.1 in the IANA JSON Web Signature and Encryption Header

Parameters registry [JWS].

4.2.1. Registry Contents

- Header Parameter Name: "iv"
- Header Parameter Usage Location(s): JWE
- Change Controller: IETF
- Specification Document(s): Section 3.1.1 of [[this document]]

- Header Parameter Name: "tag"
- Header Parameter Usage Location(s): JWE
- Change Controller: IETF
- Specification Document(s): Section 3.1.2 of [[this document]]

5. Security Considerations

The security considerations in [AES] and [NIST.800-38D] also apply to this specification.

6. Normative References

[AES] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001.

[JWA] Jones, M., "JSON Web Algorithms (JWA)", draft-ietf-jose-json-web-algorithms (work in progress), July 2013.

[JWE] Jones, M., Rescorla, E., and J. Hildebrand, "JSON Web Encryption (JWE)", draft-ietf-jose-json-web-encryption (work in progress), July 2013.

[JWS] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", draft-ietf-jose-json-web-signature (work in progress), July 2013.

[NIST.800-38D] National Institute of Standards and Technology (NIST), "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST PUB 800-38D, December 2001.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Appendix A. Document History

[[to be removed by the RFC editor before publication as an RFC]]

-01

- Represented Initialization Vector and Authentication Tag values used as header parameter values so as to be more parallel with their treatment when using AES GCM for content encryption, per working group request.

-00

- Created draft-jones-jose-aes-gcm-key-wrap.

Author's Address

Michael B. Jones
Microsoft

Email: mbj@microsoft.com
URI: http://self-issued.info/