

JOSE Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 15, 2013

M. Jones
Microsoft
June 13, 2013

Key Wrapping with AES GCM for JWE
draft-jones-jose-aes-gcm-key-wrap-00

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 December 15, 2013.

Copyright Notice

Copyright (c) 2013 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Notational Conventions	3
2.	Terminology	3
3.	Key Encryption with AES GCM	3
4.	IANA Considerations	4
4.1.	JSON Web Signature and Encryption Algorithms Registration	4
4.1.1.	Registry Contents	4
5.	Security Considerations	4
6.	Normative References	4
Appendix A.	Document History	5
Author's Address	5

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 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.

Let JWE Encrypted Key value be the concatenation of the Initialization Vector value, the Ciphertext output, and the Authentication Tag output.

During key decryption, the JWE Encrypted Key value is split into three inputs to the AES GCM decryption algorithm: the first 96 bits are the Initialization Vector value, the last 128 bits are the Authentication Tag value, and the remaining bits in between are the Ciphertext value.

Jones

Expires December 15, 2013

[Page 3]

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

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

- o Algorithm Name: "A256GCMKW"
- o Algorithm Usage Location(s): "alg"
- o Implementation Requirements: OPTIONAL
- o Change Controller: IETF
- o Specification Document(s): [Section 3](#) 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), May 2013.
- [JWE] Jones, M., Rescorla, E., and J. Hildebrand, "JSON Web Encryption (JWE)", [draft-ietf-jose-json-web-encryption](#) (work in progress), May 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.

Jones

Expires December 15, 2013

[Page 4]

[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]]

-00

- o Created [draft-jones-jose-aes-gcm-key-wrap](#).

Author's Address

Michael B. Jones
Microsoft

Email: mbj@microsoft.com

URI: <http://self-issued.info/>

