Using the AES-GMAC Algorithm with the Cryptographic Message Syntax (CMS)
                  draft-ietf-lamps-cms-aes-gmac-alg-00

Abstract

   This document specifies the conventions for using the AES-GMAC
   Message Authentication Code algorithms with the Cryptographic Message
   Syntax (CMS) as specified in RFC 5652.

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 5 June 2021.

Copyright Notice

Table of Contents

1. Introduction

   This document specifies the conventions for using the AES-GMAC
   [AES][GCM] Message Authentication Code (MAC) algorithm with the
   Cryptographic Message Syntax (CMS) [RFC5652].

2. Terminology

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
   "OPTIONAL" in this document are to be interpreted as described in
   BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
   capitals, as shown here.

3. Message Authentication Code Algorithms

   This section specifies the conventions employed by CMS [RFC5652]
   implementations that support the AES-GMAC [AES][GCM] Message
   Authentication Code (MAC) algorithm.

   MAC algorithm identifiers are located in the AuthenticatedData
   macAlgorithm field.

   MAC values are located in the AuthenticatedData mac field.

3.1. AES-GMAC

   The AES-GMAC [AES][GCM] Message Authentication Code (MAC) algorithm
   uses one of the following algorithm identifiers; the choice depends
   on the size of the AES key, which is either 128 bits, 192 bits, or
   256 bits:

```
   aes OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840)
          organization(1) gov(101) csor(3) nistAlgorithm(4) 1 }

   id-aes128-GMAC OBJECT IDENTIFIER ::= { aes 9 }

   id-aes192-GMAC OBJECT IDENTIFIER ::= { aes 29 }

   id-aes256-GMAC OBJECT IDENTIFIER ::= { aes 49 }
```

For all three of these algorithm identifier values, the
AlgorithmIdentifier parameters field MUST be present, and the
parameters MUST contain GMACParameters:

```
   GMACParameters ::= SEQUENCE {
      nonce         OCTET STRING, -- recommended size is 12 octets
      length        MACLength DEFAULT 12 }

   MACLength ::= INTEGER (12 | 13 | 14 | 15 | 16)
```

The GMACParameters nonce parameter is the GMAC initialization vector.
The nonce may have any number of bits between 8 and 2^64, but it MUST
be a multiple of 8 bits. Within the scope of any content-
authentication key, the nonce value MUST be unique. A nonce value of
12 octets can be processed more efficiently, so that length for the
nonce value is RECOMMENDED.

The GMACParameters length parameter field tells the size of the
message authentication code. It MUST match the size in octets of the
value in the AuthenticatedData mac field. A length of 12 octets is
RECOMMENDED.

4. Implementation Considerations

An implementation of the Advanced Encryption Standard (AES) Galois/
Counter Mode (GCM) authenticated encryption algorithm is specified in
[GCM]. An implementation of AES-GCM can be used to compute the GMAC
message authentication code by providing the content-authentication
key as the AES key, the nonce as the initialization vector, a zero-
length plaintext content, and the content to be authenticated as the
additional authenticated data (AAD). The result of the AES-GCM
invocation is the AES-GMAC authentication code, which is called the
authentication tag in some implementations. In AES-GCM, the
encryption step is skipped when no input plaintext is provided, and
therefore, no ciphertext is produced.

5. ASN.1 Module

   The following ASN.1 module uses the definition for MAC-ALGORITHM from
   [RFC5912].

   CryptographicMessageSyntaxGMACAlgorithms
       { iso(1) member-body(2) us(840) rsadsi(113549)
         pkcs(1) pkcs-9(9) smime(16) modules(0)
         id-mod-aes-gmac-alg-2020(TBD) }

   DEFINITIONS IMPLICIT TAGS ::=
   BEGIN

   -- EXPORTS All

   IMPORTS
     AlgorithmIdentifier{}, MAC-ALGORITHM
     FROM AlgorithmInformation-2009 -- from [RFC5912]
         { iso(1) identified-organization(3) dod(6) internet(1)
           security(5) mechanisms(5) pkix(7) id-mod(0)
           id-mod-algorithmInformation-02(58)} ;

   -- Object Identifiers

   aes OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840)
         organization(1) gov(101) csor(3) nistAlgorithm(4) 1 }

   id-aes128-GMAC OBJECT IDENTIFIER ::= { aes 9 }

   id-aes192-GMAC OBJECT IDENTIFIER ::= { aes 29 }

   id-aes256-GMAC OBJECT IDENTIFIER ::= { aes 49 }

   -- GMAC Parameters

   GMACParameters ::= SEQUENCE {
      nonce   OCTET STRING, -- recommended size is 12 octets
      length   MACLength DEFAULT 12 }

   MACLength ::= INTEGER (12 | 13 | 14 | 15 | 16)

   -- Algorithm Identifiers

   maca-aes128-GMAC MAC-ALGORITHM ::= {
      IDENTIFIER id-aes128-GMAC
      PARAMS TYPE GMACParameters ARE required
      IS-KEYED-MAC TRUE }

```
maca-aes192-GMAC MAC-ALGORITHM ::= {
    IDENTIFIER id-aes192-GMAC
    PARAMS TYPE GMACParameters ARE required
    IS-KEYED-MAC TRUE }

maca-aes256-GMAC MAC-ALGORITHM ::= {
    IDENTIFIER id-aes256-GMAC
    PARAMS TYPE GMACParameters ARE required
    IS-KEYED-MAC TRUE }

END -- of CryptographicMessageSyntaxGMACAlgorithms
```

6. IANA Considerations

IANA is asked to register object identifiers for one module
identifier in the "SMI Security for S/MIME Module Identifier
(1.2.840.113549.1.9.16.0)" registry for id-mod-aes-gmac-alg-2020.

7. Security Considerations

The CMS provides a method for authenticating data. This document
identifies the conventions for using the AES-GMAC algorithm with the
CMS.

The key management technique employed to distribute message-
authentication keys must itself provide authentication, otherwise the
content is delivered with integrity from an unknown source.

When more than two parties share the same message-authentication key,
data origin authentication is not provided. Any party that knows the
message-authentication key can compute a valid MAC, therefore the
content could originate from any one of the parties.

Within the scope of any content-authentication key, the AES-GMAC
nonce value MUST be unique. Use of a nonce value more than once
allows an attacker to generate valid AES-GMAC authentication codes
for arbitrary messages, resulting in the loss of authentication as
described in Appendix A of [GCM].

Implementations must randomly generate message-authentication keys.
The use of inadequate pseudo-random number generators (PRNGs) to
generate keys can result in little or no security. An attacker may
find it much easier to reproduce the PRNG environment that produced
the keys, searching the resulting small set of possibilities, rather
than brute force searching the whole key space. The generation of
quality random numbers is difficult. [RFC4086] offers important
guidance in this area.

Implementers should be aware that cryptographic algorithms become
weaker with time. As new cryptanalysis techniques are developed and
computing performance improves, the work factor to break a particular
cryptographic algorithm will reduce. Therefore, cryptographic
algorithm implementations should be modular allowing new algorithms
to be readily inserted. That is, implementers should be prepared to
regularly update the set of algorithms in their implementations.

8. References

8.1. Normative References

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

[GCM]   Dworkin, M., "Recommendation for Block Cipher Modes of
           Operation: Galois/Counter Mode (GCM) and GMAC", NIST
           Special Publication 800-38D, November 2007.

[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>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70,
           RFC 5652, DOI 10.17487/RFC5652, September 2009,
           <https://www.rfc-editor.org/info/rfc5652>.

[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/info/rfc8174>.

8.2. Informative References

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker,
           "Randomness Requirements for Security", BCP 106, RFC 4086,
           DOI 10.17487/RFC4086, June 2005,
           <https://www.rfc-editor.org/info/rfc4086>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the
           Public Key Infrastructure Using X.509 (PKIX)", RFC 5912,
           DOI 10.17487/RFC5912, June 2010,
           <https://www.rfc-editor.org/info/rfc5912>.

Author's Address

   Russ Housley
   Vigil Security, LLC
   516 Dranesville Road
   Herndon, VA, 20170
   United States of America

   Email: housley@vigilsec.com