

TCPM Working Group  
Internet-Draft  
Updates: RFC 5926 (if approved)  
Intended status: Standards Track  
Expires: 3 October 2026

R. Bonica  
T. Li  
HPE  
1 April 2026

Additional Security Algorithms For Use With TCP-AO  
draft-bonica-tcpm-tcp-ao-algs-01

## Abstract

RFC5926 specifies cryptographic algorithms for TCP-AO. It explains how to use KDF\_HMAC\_SHA1 and KDF\_AES\_128\_CMAC as KDFs. It also explains how to use HMAC-SHA-1-96 and AES-128-CMAC-96 as MAC algorithms.

This document specifies several new KDFs and MAC algorithms for TCP-AO. The KDFs and MAC algorithms specified in this document use stronger cryptography.

## 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 3 October 2026.

## Copyright Notice

Copyright (c) 2026 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 (<https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Conventions and Definitions . . . . .	4
3. Updates to RFC 5926 . . . . .	4
3.1. Concrete KDFs . . . . .	4
3.1.1. KDF_HMAC_SHA256 . . . . .	4
3.1.2. KDF_HMAC_SHA384 . . . . .	4
3.1.3. KDF_HMAC_SHA512 . . . . .	5
3.1.4. KDF_HMAC_SHA3-256 . . . . .	5
3.1.5. KDF_HMAC_SHA3-384 . . . . .	5
3.1.6. KDF_HMAC_SHA3-512 . . . . .	6
3.2. MAC Algorithms . . . . .	6
3.2.1. The Use of HMAC-SHA256-128 . . . . .	6
3.2.2. The Use of HMAC-SHA384-128 . . . . .	7
3.2.3. The Use of HMAC-SHA512-128 . . . . .	7
3.2.4. The Use of HMAC-SHA3-256-128 . . . . .	8
3.2.5. The Use of HMAC-SHA3-384-128 . . . . .	9
3.2.6. The Use of HMAC-SHA3-512-128 . . . . .	9
4. Security Considerations . . . . .	10
5. IANA Considerations . . . . .	10
6. Acknowledgements . . . . .	11
7. Normative References . . . . .	11
Authors' Addresses . . . . .	12

## 1. Introduction

TCP end-points use the TCP Authentication Option (TCP-AO) [RFC5925] to authenticate segments. TCP-AO relies upon:

- \* A Master Key Tuple (MKT)
- \* A Key Derivation Function (KDF)
- \* A Message Authentication Code (MAC) algorithm

TCP-AO systems are configured with one or more MKTs for each connection that they protect. When a connection is associated with multiple MKTs, TCP-AO can rotate among them during the course of a TCP session. This facilitates dynamic key change and authentication algorithm agility.

An MKT includes:

- \* Two MKT identifiers, one used for sending and one used for receiving
- \* A connection identifier (i.e., a TCP socket pair)
- \* A master key (i.e., a shared secret)
- \* A KDF
- \* A MAC algorithm
- \* A flag indicating whether TCP options other than TCP-AO are authenticated

The KDF generates a traffic key. Its inputs are:

- \* A pseudorandom function (PRF) used to generate the traffic key
- \* The master key
- \* Context (i.e., A binary string containing information related to the connection)
- \* Output length (i.e., the length of the traffic key, in bits)

The MAC algorithm produces a MAC. It is defined by:

- \* The KDF algorithm used to generate the traffic key
- \* The length of the traffic key, in bits
- \* The length of the MAC, in bits

The following are inputs to the MAC Algorithm:

- \* traffic key
- \* message

TCP-AO systems include the MAC in the TCP-AO. They use the MAC to authenticate segments.

[RFC5926] specifies cryptographic algorithms for TCP-AO. It explains how to use KDF\_HMAC\_SHA1 and KDF\_AES\_128\_CMAC as KDFs. It also explains how to use HMAC-SHA-1-96 and AES-128-CMAC-96 as MAC algorithms.

This document specifies several new KDFs and MAC algorithms for TCP-AO. The KDFs and MAC algorithms defined in this document use stronger cryptography.

According to [RFC2104], "Applications of HMAC can choose to truncate the output of HMAC by outputting the  $t$  leftmost bits of the HMAC computation for some parameter  $t$ ".

The algorithms described in this document truncate the output of HMAC to 128 bits (i.e., 16 bytes). Therefore, when they are encoded in TCP-AO, the TCP-AO consumes 20 bytes.

## 2. Conventions and Definitions

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 BCP14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. Updates to RFC 5926

### 3.1. Concrete KDFs

#### 3.1.1. KDF\_HMAC\_SHA256

For KDF\_HMAC\_SHA256:

- \* PRF for KDF\_alg: HMAC-SHA256 [RFC2104]  
[DOI.10.6028\_NIST.FIPS.180-4]
- \* Use: HMAC-SHA256(Key, Input).
- \* Input: (  $i$  || Label || Context || Output\_Length)
- \* Key: Master\_Key, configured by user, and passed to the KDF
- \* Output\_Length: 256 bits
- \* Result: Traffic\_Key, used in the MAC function by TCP-AO

#### 3.1.2. KDF\_HMAC\_SHA384

For KDF\_HMAC\_SHA384:

- \* PRF for KDF\_alg: HMAC-SHA384 [RFC2104]  
[DOI.10.6028\_NIST.FIPS.180-4]

- \* Use: HMAC-SHA384(Key, Input).
- \* Input: ( i || Label || Context || Output\_Length)
- \* Key: Master\_Key, configured by user, and passed to the KDF
- \* Output\_Length: 384 bits
- \* Result: Traffic\_Key, used in the MAC function by TCP-AO

#### 3.1.3. KDF\_HMAC\_SHA512

For KDF\_HMAC\_SHA512:

- \* PRF for KDF\_alg: HMAC-SHA512 [RFC2104]  
[DOI.10.6028\_NIST.FIPS.180-4]
- \* Use: HMAC-SHA512(Key, Input).
- \* Input: ( i || Label || Context || Output\_Length)
- \* Key: Master\_Key, configured by user, and passed to the KDF
- \* Output\_Length: 512 bits
- \* Result: Traffic\_Key, used in the MAC function by TCP-AO

#### 3.1.4. KDF\_HMAC\_SHA3-256

For KDF\_HMAC\_SHA3-256:

- \* PRF for KDF\_alg: HMAC-SHA3-256 [RFC2104]  
[DOI.10.6028\_NIST.FIPS.202]
- \* Use: HMAC-SHA3-256(Key, Input).
- \* Input: ( i || Label || Context || Output\_Length)
- \* Key: Master\_Key, configured by user, and passed to the KDF
- \* Output\_Length: 256 bits
- \* Result: Traffic\_Key, used in the MAC function by TCP-AO

#### 3.1.5. KDF\_HMAC\_SHA3-384

For KDF\_HMAC\_SHA3-384:

- \* PRF for KDF\_alg: HMAC-SHA3-384 [RFC2104]  
[DOI.10.6028\_NIST.FIPS.202]
- \* Use: HMAC-SHA3-384(Key, Input).
- \* Input: ( i || Label || Context || Output\_Length)
- \* Key: Master\_Key, configured by user, and passed to the KDF
- \* Output\_Length: 384 bits
- \* Result: Traffic\_Key, used in the MAC function by TCP-AO

### 3.1.6. KDF\_HMAC\_SHA3-512

For KDF\_HMAC\_SHA3-512:

- \* PRF for KDF\_alg: HMAC-SHA3-512 [RFC2104]  
[DOI.10.6028\_NIST.FIPS.202]
- \* Use: HMAC-SHA3-512(Key, Input).
- \* Input: ( i || Label || Context || Output\_Length)
- \* Key: Master\_Key, configured by user, and passed to the KDF
- \* Output\_Length: 512 bits
- \* Result: Traffic\_Key, used in the MAC function by TCP-AO

## 3.2. MAC Algorithms

The following subsections should be added to Section 3.2 of [RFC5926].

### 3.2.1. The Use of HMAC-SHA256-128

By definition, HMAC [RFC2104] requires a cryptographic hash function. SHA256 will be that hash function used for authenticating and providing integrity validation on TCP segments with HMAC.

The three fixed elements for HMAC-SHA256-128 are:

- \* KDF\_Alg: KDF\_HMAC\_SHA256
- \* Key\_Length: 256 bits.
- \* MAC\_Length: 128 bits.

For:

- \* `MAC = MAC_alg (Traffic_Key, Message)`

HMAC-SHA256-128 for TCP-AO has the following values:

- \* `MAC_alg`: HMAC-SHA256
- \* `Traffic_Key`: Variable; the result of the KDF.
- \* `Message`: The message to be authenticated, as specified in [RFC5925], Section 5.1.

### 3.2.2. The Use of HMAC-SHA384-128

By definition, HMAC [RFC2104] requires a cryptographic hash function. SHA384 will be that hash function used for authenticating and providing integrity validation on TCP segments with HMAC.

The three fixed elements for HMAC-SHA384-128 are:

- \* `KDF_Alg`: `KDF_HMAC_SHA384`
- \* `Key_Length`: 384 bits.
- \* `MAC_Length`: 128 bits.

For:

- \* `MAC = MAC_alg (Traffic_Key, Message)`

HMAC-SHA384-128 for TCP-AO has the following values:

- \* `MAC_alg`: HMAC-SHA384
- \* `Traffic_Key`: Variable; the result of the KDF.
- \* `Message`: The message to be authenticated, as specified in [RFC5925], Section 5.1.

### 3.2.3. The Use of HMAC-SHA512-128

By definition, HMAC [RFC2104] requires a cryptographic hash function. SHA512 will be that hash function used for authenticating and providing integrity validation on TCP segments with HMAC.

The three fixed elements for HMAC-SHA512-128 are:

- \* KDF\_Alg: KDF\_HMAC\_SHA512
- \* Key\_Length: 512 bits.
- \* MAC\_Length: 128 bits.

For:

- \* MAC = MAC\_alg (Traffic\_Key, Message)

HMAC-SHA512-128 for TCP-AO has the following values:

- \* MAC\_alg: HMAC-SHA512
- \* Traffic\_Key: Variable; the result of the KDF.
- \* Message: The message to be authenticated, as specified in [RFC5925], Section 5.1.

#### 3.2.4. The Use of HMAC-SHA3-256-128

By definition, HMAC [RFC2104] requires a cryptographic hash function. SHA3-256 will be that hash function used for authenticating and providing integrity validation on TCP segments with HMAC.

The three fixed elements for HMAC-SHA3-256-128 are:

- \* KDF\_Alg: KDF\_HMAC\_SHA3-256.
- \* Key\_Length: 256 bits.
- \* MAC\_Length: 128 bits.

For:

- \* MAC = MAC\_alg (Traffic\_Key, Message)

HMAC-SHA3-256-128 for TCP-AO has the following values:

- \* MAC\_alg: HMAC-SHA3-256.
- \* Traffic\_Key: Variable; the result of the KDF.
- \* Message: The message to be authenticated, as specified in [RFC5925], Section 5.1.



### 3.2.5. The Use of HMAC-SHA3-384-128

By definition, HMAC [RFC2104] requires a cryptographic hash function. SHA3-384 will be that hash function used for authenticating and providing integrity validation on TCP segments with HMAC.

The three fixed elements for HMAC-SHA3-384-128 are:

- \* KDF\_Alg: KDF\_HMAC\_SHA3-384.
- \* Key\_Length: 384 bits.
- \* MAC\_Length: 128 bits.

For:

- \* MAC = MAC\_alg (Traffic\_Key, Message)

HMAC-SHA3-384-128 for TCP-AO has the following values:

- \* MAC\_alg: HMAC-SHA3-384.
- \* Traffic\_Key: Variable; the result of the KDF.
- \* Message: The message to be authenticated, as specified in [RFC5925], Section 5.1.

### 3.2.6. The Use of HMAC-SHA3-512-128

By definition, HMAC [RFC2104] requires a cryptographic hash function. SHA3-512 will be that hash function used for authenticating and providing integrity validation on TCP segments with HMAC.

The three fixed elements for HMAC-SHA3-512-128 are:

- \* KDF\_Alg: KDF\_HMAC\_SHA3-512.
- \* Key\_Length: 512 bits.
- \* MAC\_Length: 128 bits.

For:

- \* MAC = MAC\_alg (Traffic\_Key, Message)

HMAC-SHA3-512-128 for TCP-AO has the following values:

- \* MAC\_alg: HMAC-SHA3-512.

- \* Traffic\_Key: Variable; the result of the KDF.
- \* Message: The message to be authenticated, as specified in [RFC5925], Section 5.1.

#### 4. Security Considerations

According to [RFC2104], "Applications of HMAC can choose to truncate the output of HMAC by outputting the  $t$  leftmost bits of the HMAC computation for some parameter  $t$ ".

The algorithms described in this document truncate the output of HMAC to 128 bits (i.e., 16 bytes). Therefore, when they are encoded in TCP-AO, the TCP-AO consumes 20 bytes.

[RFC2104] continues, "We recommend that the output length  $t$  be not less than half the length of the hash output (to match the birthday attack bound) and not less than 80 bits (a suitable lower bound on the number of bits that need to be predicted by an attacker)".

In this document, only the following MAC algorithms comply with that recommendation:

- \* HMAC-SHA256-128
- \* HMAC-SHA3-256-128

#### 5. IANA Considerations

IANA is requested to add the following entries to the "Cryptographic Algorithms for TCP-AO Registration" (<https://www.iana.org/assignments/tcp-parameters/tcp-parameters.xhtml#tcp-parameters-3>).

Algorithm	Reference
SHA256-128	This Document
SHA384-128	This Document
SHA512-128	This Document
SHA3-256-128	This Document
SHA3-384-128	This Document
SHA3-512-128	This Document

Table 1: IANA Actions

## 6. Acknowledgements

Thanks to Lars Eggert, Gorrry Fairhurst, C.M. Heard, Russ Housley, John Mattsson, Yoshifumi Nishida, Joe Touch, Michael Tuxen, and Magnus Westerlund for their review and comments.

## 7. Normative References

- [DOI.10.6028\_NIST.FIPS.180-4]  
 "Secure hash standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.180-4, 2015, <<https://doi.org/10.6028/nist.fips.180-4>>.
- [DOI.10.6028\_NIST.FIPS.197]  
 "Advanced Encryption Standard (AES)", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.197, 2001, <<https://doi.org/10.6028/nist.fips.197>>.
- [DOI.10.6028\_NIST.FIPS.202]  
 "SHA-3 standard :: permutation-based hash and extendable-output functions", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.202, 2015, <<https://doi.org/10.6028/nist.fips.202>>.

- [DOI.10.6028\_NIST.SP.800-38B]  
Dworkin, M., "Recommendation for block cipher modes of operation :: the CMAC mode for authentication", National Institute of Standards and Technology, DOI 10.6028/nist.sp.800-38b, 2016, <<https://doi.org/10.6028/nist.sp.800-38b>>.
- [RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <<https://www.rfc-editor.org/rfc/rfc2104>>.
- [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>>.
- [RFC4615] Song, J., Poovendran, R., Lee, J., and T. Iwata, "The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4615, DOI 10.17487/RFC4615, August 2006, <<https://www.rfc-editor.org/rfc/rfc4615>>.
- [RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <<https://www.rfc-editor.org/rfc/rfc5925>>.
- [RFC5926] Lebovitz, G. and E. Rescorla, "Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)", RFC 5926, DOI 10.17487/RFC5926, June 2010, <<https://www.rfc-editor.org/rfc/rfc5926>>.
- [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>>.

## Authors' Addresses

Ron Bonica  
HPE  
United States of America  
Email: [ronald.bonica@hpe.com](mailto:ronald.bonica@hpe.com)

Tony Li  
HPE  
United States of America

Email: [tony.li@tony.li](mailto:tony.li@tony.li)