

TCPM
Internet-Draft
Intended status: Standards Track
Expires: August 14, 2010

G. Lebovitz
Juniper
E. Rescorla
RTFM
February 10, 2010

Cryptographic Algorithms for TCP's Authentication Option, TCP-AO
draft-ietf-tcpm-tcp-ao-crypto-02

Abstract

The TCP Authentication Option, TCP-AO, relies on security algorithms to provide authentication between two end-points. There are many such algorithms available, and two TCP-AO systems cannot interoperate unless they are using the same algorithms. This document specifies the algorithms and attributes that can be used in TCP-AO's current manual keying mechanism.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 14, 2010.

Copyright Notice

Copyright (c) 2010 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

Internet-Draft

Crypto for TCP-A0

February 2010

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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Draft

Crypto for TCP-A0

February 2010

Table of Contents

- [1. Introduction](#) [4](#)
- [2. Requirements](#) [4](#)
 - [2.1. Requirements Language](#) [4](#)
 - [2.2. Algorithm Requirements](#) [4](#)
 - [2.3. Requirements for Future MAC Algorithms](#) [5](#)
- [3. Algorithms Specified](#) [5](#)
 - [3.1. Key Derivation Functions \(KDFs\)](#) [6](#)
 - [3.1.1. Concrete KDFs](#) [7](#)
 - [3.2. MAC Algorithms](#) [11](#)
 - [3.2.1. The Use of HMAC-SHA-1-96](#) [12](#)
 - [3.2.2. The Use of AES-128-CMAC-96](#) [12](#)
- [4. Change History \(RFC Editor: Delete before publishing\) . . .](#) [13](#)
- [5. Needs Work in Next Draft \(RFC Editor: Delete Before Publishing\)](#) [15](#)
- [6. Security Considerations](#) [15](#)
- [7. IANA Considerations](#) [16](#)
- [8. Acknowledgements](#) [17](#)
- [9. References](#) [17](#)
 - [9.1. Normative References](#) [17](#)
 - [9.2. Informative References](#) [18](#)
- [Authors' Addresses](#) [19](#)

1. Introduction

This document is a companion to [TCP-AO] [[I-D.ietf-tcpm-tcp-auth-opt](#)]. Like most modern security protocols, TCP-AO allows users to chose which cryptographic algorithm(s) they want to use to meet their security needs.

TCP-AO provides cryptographic authentication and message integrity verification between to end-points. In order to accomplish this function, message authentication codes (MACs) are used, which then rely on shared keys. There are various ways to create MACs. The use of hashed-based MACs (HMAC) in Internet protocols is defined in [[RFC2104](#)]. The use of cipher-based MACs (CMAC) in Internet protocols is defined in [[RFC4493](#)].

This RFC defines the general requirements for MACs used in TCP-AO, both for currently specified MACs and for any future specified MACs. It then specifies two MAC algorithms required in all TCP-AO implementations. It also specifies two key derivation functions (KDFs) used to create the traffic keys used by the MACs. These KDFs are also required by all TCP-AO implementations.

2. Requirements

2.1. Requirements Language

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](#)].

When used in lower case, these words convey their typical use in common language, and are not to be interpreted as described in [[RFC2119](#)].

[2.2.](#) Algorithm Requirements

This is the initial specification of required cryptography for TCP-A0, and indicates two MAC algorithms and two KDFs. All four components MUST be implemented in order for the implementation to be fully compliant with this RFC.

The following table indicates the required MAC algorithms and KDFs for TCP-A0:

Requirement	Authentication Algorithm
MUST	HMAC-SHA-1-96 [RFC2404]
MUST	AES-128-CMAC-96 [RFC4493]
Requirement	Key Derivation Function (KDF)
MUST	KDF_HMAC_SHA1
MUST	KDF_AES_128_CMAC

NOTE EXPLAINING WHY TWO MAC ALGORITHMS WERE MANDATED:

Two MAC algorithms and two corresponding KDFs are mandated as a result of discussion in the TCPM WG, and in consultation with the Security Area Directors. SHA-1 was selected because it is widely deployed and currently has sufficient strength and reasonable computational cost, so it is a "MUST" for TCP-A0 today. The security strength of SHA-1 HMACs should be sufficient for the foreseeable future, especially given that the tags are truncated to 96 bits.

Recently exposed vulnerabilities in other MACs (e.g., MD5 or HMAC MD5) aren't practical on SHA-1, but these types of analyses are mounting and could potentially pose a concern for HMAC forgery if they were significantly improved, over time. The security issues driving the migration from SHA-1 to SHA-256 for digital signatures [[HMAC-ATTACK](#)] do not immediately render SHA-1 weak for this application of SHA-1 in HMAC mode.

AES-128 CMAC is considered to be a stronger algorithm than SHA-1, but may not yet have very wide implementation. AES-128 CMAC is also a "MUST" to implement, in order to drive vendors toward its use, and to allow for another MAC option, if SHA-1 were to be compromised.

[2.3.](#) Requirements for Future MAC Algorithms

TCP-AO is intended to support cryptographic agility. As a result, this document includes recommendations in various places for future MAC and KDF algorithms when used for TCP-AO. For future MAC algorithms specifically, they SHOULD protect at least 2^{48} messages with a collision probability of less than one in 10^9 .

[Reviewers: Are there any other requirements we want/need to place in here? RFC EDITOR: Please delete this note before publishing as RFC]

[3.](#) Algorithms Specified

TCP-AO requires two classes of cryptographic algorithms used on a

particular connection, and refers to this document to define them both:

- (1) Key Derivation Functions (KDFs) which name a pseudorandom function (PRF) and use a Master_Key and some connection-specific input with that PRF to produce Traffic_Keys, the keys suitable for authenticating and integrity checking individual TCP segments, as described in TCP-AO.
- (2) Message Authentication Code (MAC) algorithms which take a key and a message and produce an authentication tag which can be used to verify the integrity and authenticity of those messages.

In TCP-A0, these algorithms are always used in pairs. Each MAC algorithm MUST specify the KDF to be used with that MAC algorithm. However, a KDF MAY be used with more than one MAC algorithm.

3.1. Key Derivation Functions (KDFs)

TCP-A0's Traffic_Keys are derived using KDFs. The KDFs used in TCP-A0's current manual keying have the following interface:

$$\text{Traffic_Key} = \text{KDF_alg}(\text{Master_Key}, \text{Context}, \text{Output_Length})$$

where:

- KDF_alg: the specific pseudorandom function (PRF) that is the basic building block used in constructing the given Traffic_Key.
- Master_Key: In TCP-A0's manual key mode, this is a key shared by both peers, entered via some interface to their respective configurations. The Master_Key is used as the seed for the KDF. We assume that this is a human-readable pre-shared key (PSK), thus we assume it is of variable length. Master_Keys SHOULD be random, but might not be (e.g., badly chosen by the user).
- Context : A binary string containing information related to the specific connection for this derived keying material, as defined in [\[I-D.ietf-tcpm-tcp-auth-opt\]](#), Section 7.2]

- Output_Length: The length in bits of the key that the KDF will produce. This length must be the size required for the MAC algorithm that will use the PRF result as a seed.

When invoked, a KDF generates a string of length `Output_Length` bits based on `Master_Key` and context value. This result may then be used as a cryptographic key for any algorithm which takes an `Output_Length` length key. A KDF MAY specify a maximum `Output_Length` parameter.

[3.1.1.](#) Concrete KDFs

This document defines two KDF algorithms, each paired with a corresponding PRF algorithm as explained below:

- * `KDF_HMAC_SHA1` based on PRF-HMAC-SHA1 [[RFC2404](#)]
- * `KDF_AES_128_CMAC` based on AES-CMAC-PRF-128 [[RFC4615](#)]

Both of these KDFs are based on the iteration mode KDFs specified in [[NIST-SP800-108](#)]. This means that they use an underlying pseudorandom function (PRF) with a fixed-length output lengths, 128 bits in the case of the AES-CMAC, and 160 bits in the case of HMAC-SHA1. The KDF generates an arbitrary number of output bits by operating the PRF in a "counter mode", where each invocation of the PRF uses a different input block differentiated by a block counter.

Each input block is constructed as follows:

`(i || Label || Context || Output_Length)`

Where

- `"||"`: For any `X || Y`, `"||"` represents a concatenation operation of the binary strings `X` and `Y`.
- `i`: A counter, a binary string that is an input to each iteration of the PRF in counter mode. The counter `"i"` is represented in a single octet. The number of iterations will depend on the specific size of the `Output_Length` desired for a given MAC. `"i"` always starts = 1.

- Label: A binary string that clearly identifies the purpose of this KDF's derived keying material. For TCP-A0 we use the ASCII string "TCP-A0", where the last character is the capital letter "0", not to be confused with a zero. While this may seem like overkill in this specification since TCP-A0 only describes one call to the KDF, it is included in order to comply with FIPS 140 certifications.
- Context : The context argument provided to the KDF interface, as described above in [Section 3.1](#) .
- Output_Length: The length in bits of the key that the KDF will produce. The Output_length is represented within two octets. This length must be the size required for the MAC algorithm that will use the PRF result as a seed.

The output of multiple PRF invocations is simply concatenated. For the Traffic_Key, values of multiple PRF invocations are concatenated and truncated as needed to create a Traffic_Key of the desired length. For instance, if one were using KDF_HMAC_SHA1, which uses a 160-bit internal PRF to generate 320 bits of data, one would execute the PRF twice, once with i=1 and once with i=2. The result would be the entire output of the first invocation concatenated with the second invocation. E.g.,

```
Traffic_Key =
    KDF_alg(Master_Key, 1 || Label || Context || Output_length) ||
    KDF_alg(Master_Key, 2 || Label || Context || Output_length)
```

If the number of bits required is not an even multiple of the output size of the PRF, then the output of the final invocation of the PRF is truncated as necessary.

[3.1.1.1](#). KDF_HMAC_SHA1

For KDF_HMAC_SHA1:

- PRF for KDF_alg: HMAC-SHA1 [[RFC2404](#)].
- Use: HMAC-SHA1(Key, Input).

Internet-Draft

Crypto for TCP-A0

February 2010

- Key: Master_Key, configured by user, and passed to the KDF.
- Input: (i || Label || Context || Output_Length)
- Output_Length: 160 bits.
- Result: Traffic_Key, used in the MAC function by TCP-A0.

[3.1.1.2.](#) KDF_AES_128_CMAC

For KDF_AES_128_CMAC:

- PRF for KDF_alg: AES-CMAC-PRF-128 [[RFC4615](#)].
- Use: AES-CMAC(Key, Input).
- Key: Master_Key (see usage below)
- Input: (i || Label || Context || Output_Length)
- Output_Length: 128 bits.
- Result: Traffic_Key, used in the MAC function by TCP-A0

The Master_Key in TCP-A0's current manual keying mechanism is a shared secret, entered by an administrator. It is passed via an out-of-band mechanism between two devices, and often between two organizations. The shared secret does not have to be 16 octets, and the length may vary. However, AES_128_CMAC requires a key of exactly 16 octets (128 bits) in length. We could mandate that implementations force administrators to input Master_Keys of exactly 128 bit length when using AES_128_CMAC, and with sufficient randomness, but this places undue burden on the implementors and deployers. This specification RECOMMENDS that deployers use a randomly generated 128-bit string as the Master_Key, but acknowledges that deployers may not.

To handle variable length Master_Keys we use the same mechanism as described in [[RFC4615](#)], Sect 3. First we use AES_128_CMAC with a fixed key of all zeros as a "randomness extractor", while using the shared secret Master_Key, MK, as the message input, to produce a 128 bit key Derived_Master_Key (K). Second, we use the result as a key, and run AES-128_CMAC again, this time using the result K as the Key,

and the true input block as the Input to yield the Traffic_Key (TK) used in the MAC over the message. The description follows:

```
+++++
+                               KDF-AES-128-CMAC                               +
+++++
+                               +
+ Input  : MK (Master_Key, the variable-length shared secret)             +
+       : I (Input, i.e., the input data of the PRF)                       +
+       : MKlen (length of MK in octets)                                    +
+       : len (length of M in octets)                                       +
+ Output : TK (Traffic_Key, 128-bit Pseudo-Random Variable)              +
+                               +
+-----+
+ Variable: K (128-bit key for AES-CMAC)                                    +
+                               +
+ Step 1.  If MKlen is equal to 16                                         +
+ Step 1a. then                                                            +
+         K := MK;                                                         +
+ Step 1b. else                                                            +
+         K := AES-CMAC(0^128, MK, MKlen);                                  +
+ Step 2.  TK := AES-CMAC(K, I, len);                                       +
+         return TK;                                                       +
+                               +
+++++
```

Figure 1

In step 1, the 128-bit key, K, for AES-CMAC is derived as follows:

- o If the Master_Key, MK, provided by the administrator is exactly 128 bits, then we use it as-is.
- o If it is longer or shorter than 128 bits, then we derive the key K by applying the AES-CMAC algorithm using the 128-bit all-zero string as the key and MK as the input message. This step is described in step 1b.

In step 2, we apply the AES-CMAC algorithm again, this time using K as the key and I as the input message.

The output of this algorithm returns TK, the Traffic_Key, which is 128 bits suitable for use in the MAC function on each TCP segment of the connection.

[3.1.1.3](#). Tips for User Interfaces regarding KDFs

This section provides suggested representations for the KDFs in implementation user interfaces. Following these guidelines across common implementations will make interoperability easier and simpler

for deployers.

UIs SHOULD refer to the choice of KDF_HMAC_SHA1 as simply "SHA1".

UIs SHOULD refer to the choice of KDF_AES_128_CMAC as simply "AES128".

The initial IANA registry values will reflect these two entries.

UIs SHOULD use KDF_HMAC_SHA1 as the default selection in TCP-AO settings. KDF_HMAC_SHA1 is preferred at this time because it has wide support, being present in most implementations in the marketplace.

[3.2](#). MAC Algorithms

Each MAC_alg defined for TCP-AO has three fixed elements as part of its definition:

- KDF_Alg: Name of the TCP-AO KDF algorithm used to generate the Traffic_Key
- Key_Length: Length in bits required for the Traffic_Key used in this MAC
- MAC_Length: The final length of the bits used in the TCP-AO MAC field. This value may be a truncation of the MAC function's original output length.

MACs computed for TCP-AO have the following interface:

MAC = MAC_alg(Traffic_Key, Message)

where:

- MAC_alg: MAC Algorithm used
- Traffic_Key: Variable; the result of KDF.
- Message The message to be authenticated, as specified in [\[I-D.ietf-tcpm-tcp-auth-opt\] Section 7.1](#).

This document specifies two MAC algorithm options for generating the MAC as used by TCP-AO:

- * HMAC-SHA-1-96 based on [\[RFC2404\]](#)

- * AES-128-CMAC-96 based on [\[RFC4493\]](#)

Both provide a high level of security and efficiency. The AES-128-CMAC-96 is potentially more efficient, particularly in hardware, but HMAC-SHA-1-96 is more widely used in Internet protocols and in most cases could be supported with little or no additional code in today's deployed software and devices.

An important aspect to note about these algorithms' definitions for use in TCP-AO is the fact that the MAC outputs are truncated to 96 bits. AES-128-CMAC-96 produces a 128 bit MAC, and HMAC SHA-1 produces a 160 bit result. The MAC output are then truncated to 96 bits to provide a reasonable tradeoff between security and message size, for fitting into the TCP-AO header.

[3.2.1](#). The Use of HMAC-SHA-1-96

By definition, HMAC [\[RFC2104\]](#) requires a cryptographic hash function. SHA1 will be that has function used for authenticating and providing integrity validation on TCP segments with HMAC.

The three fixed elements for HMAC-SHA-1-96 are:

- KDF_Alg: KDF_HMAC_SHA1.
- Key_Length: 160 bits.
- MAC_Length: 96 bits.

For:

MAC = MAC_alg (Traffic_Key, Message)

HMAC-SHA-1-96 for TCP-A0 has the following values:

- MAC_alg: HMAC-SHA1
- Traffic_Key: Variable; the result of the KDF.
- Message: The message to be authenticated, as specified in [\[I-D.ietf-tcpm-tcp-auth-opt\] Section 7.1](#).

[3.2.2.](#) The Use of AES-128-CMAC-96

In the context of TCP-A0, when we say "AES-128-CMAC-96" we actually define a usage of AES-128 as a cipher-based MAC according to [\[NIST-SP800-38B\]](#).

The three fixed elements for AES-128-CMAC-96 are:

- KDF_Alg: KDF_AES_128_CMAC.
- Key_Length: 128 bits.
- MAC_Length: 96 bits.

For:

MAC = MAC_alg (Traffic_Key, Message)

AES-128-CMAC-96 for TCP-A0 has the following values:

- MAC_alg: AES-128-CMAC-96 [\[RFC4493\]](#)

- Traffic_Key: Variable; the result of the KDF.
- Message: The message to be authenticated, as specified in [\[I-D.ietf-tcpm-tcp-auth-opt\] Section 7.1.](#)

4. Change History (RFC Editor: Delete before publishing)

[NOTE TO RFC EDITOR: this section for use during I-D stage only. Please remove before publishing as RFC.]

[draft-ietf...-02](#) - 6th submission

- o 3.1.1.1 & 3.1.1.2, s/PRF:/PRF for KDF_alg: for clarification
- o editorial touch ups - Wes
- o in 3.2 s/Output/MAC_length , because -auth-opt-10 used "Output" in a more generic way in 7.1, so the same term had two different meanings, one in each doc. Changing -ao-crypto to use MAC_length seemed most expedient.
- o in 3.1.1, changed "i" to always start = 1, and changed the concatenation example accordingly (it was starting = 0, which did not match NIST SP 800-108 - Brian Weis
- o in 3.1.1, added to definition of "i", "The counter "i" is represented in a single octet. ", and to the definition of "Output_Length" "The Output_length is represented within two octets." - Brian Weis

[draft-ietf...-01](#) - 5th submission

- o simplified title of document - Touch

- o structure of sect 3 changed: 3.1 becomes "Concrete KDF's" and the description of the two KDF's became 3.1.1.1 & 3.1.1.2. used a template (of sorts) in both sections that can be easily re-used by any future KDF definition.
- o in 3.1, switched "Derived_Key" back to "Traffic_Key" in order to sync with -auth-opt spec.
- o in 3.1, for Traffic_Key definition, changed the name of the element "Input" to "Context", and removed the hard binding to

NIST-SP800-108 at the generic interface level. The NIST inclusion is still present in the concrete definitions of the two presented KDF's, but this way, if NIST changes, or if the community wants to define some other, non-NIST-like KDFs, the interface is flexible enough to handle that. Changed "KDF" to "KDF-*alg*".

- o in 3.2, clarified that the output of the function is called "MAC =", to have a similar look and feel to sect 3.1's function. also changed MAC(*foo*) to "MAC-*alg*", and dropped "Output_Length" from the function parameters, as it is specified as a fixed element for each MAC defined, but not passed as a parameter of the function.
- o sect 3.2 - removed "truncation" from interface definition, and placed it as a fixed element of the MAC definition. sect 3.2.1 and 3.2.2 - changed "truncation:" field to "Output:". Removed text about [RFC4493](#) from end of 3.2.2.
- o sect 3.1.1.2, changed back to follow 4615 exactly (agreement with polk, mcgrew, lebovitz, ekr)
- o sect 3.1.1.3, deleted the following: "When such a time arrives as KDF_AES_128_CMAC becomes widely deployed, this document should be updated so that it becomes the default KDF on implementations."
- o added the two IANA values SHA1 and AES128 to IANA section
- o Minor text change in [section 3.1](#) and 3.2, to the definition of "Context" in both - Joe Touch
- o minor text change in 3.1.1 clarifying that the concatenation is of binary strings - Joe Touch
- o copy edits for read-ability throughout - Touch

[draft-ietf...-00](#) - 4th submission

- o Submitting [draft-lebovitz...-02](#) as a WG document. Added EKR as co- author, and gave him credit for rewrite of sect 3.1.x .

[draft-lebovitz...-02](#) - 3rd submission

- o cleaned up explanation in 3.1.2
- o in 3.1.2, changed the key extractor mechanism back, from using an alphanumeric string for the fixed key C to use 0^{^128} as the key (as it was in -00) (Polk & Ekr)
- o deleted cut-and-paste error text from sect 3.1 between "label" and "context"

- o changed "conn_key" to "traffic_key" throughout, to follow auth-

- opt-05
- o changed "tsad" to "mkt" throughout, to follow auth-opt-05
- o changed "conn_block" to "data_block" throughout, to follow auth-opt-05

[draft-lebovitz...-01](#) - 2nd submission

- o removed the whole section on labels (previously [section 4](#)), per WG consensus at IETF74. Added 3.1.3 to specify that implementations SHOULD make HMAC-SHA1 the default choice for the time being, and to suggest common names for the KDF's universally in UI's.
- o changed KDF = PRF... to Derived_Key = KDF... (EKR)
- o added the text on how to deal with future KDF to end of s3.1 (EKR)
- o removed references to TCP-A0 "manual key mode". Changed to TCP-A0's "current mode of manual keying". (Touch)
- o removed the whole MUST- / SHOULD+ thing. Both KDF's are MUST now, per wg consensus at ietf74.
- o in 3.1.2, changed the mechanism to force the K to be 128bits from using 0^{128} , to using a fixed 128-bit string of random characters (Dave McGrew)
- o sect 3.1, in Input description, dropped "0x00". Added "NOTE" explaining why right after the output_length description.
- o cleaned up all references
- o copy editing

[draft-lebovitz...-00](#) - original submission

[5.](#) Needs Work in Next Draft (RFC Editor: Delete Before Publishing)

[NOTE TO RFC EDITOR: this section for use during I-D stage only. Please remove before publishing as RFC.]

List of stuff that still needs work

- o None. ready IESG review.
- o Could use a bit broader security area review. Will ask a few folks to review.

[6.](#) Security Considerations

This document inherits all of the security considerations of the TCP-A0, the AES-CMAC, and the HMAC-SHA-1 documents.

The security of cryptographic-based systems depends on both the strength of the cryptographic algorithms chosen and the strength of the keys used with those algorithms. The security also depends on

the engineering of the protocol used by the system to ensure that there are no non-cryptographic ways to bypass the security of the overall system.

Care should also be taken to ensure that the selected key is unpredictable, avoiding any keys known to be weak for the algorithm in use.][\[RFC4086\]](#) contains helpful information on both key generation techniques and cryptographic randomness.

Note that in the composition of KDF_AES_128_CMAC, the PRF needs a 128 bit / 16 byte key as the seed. However, for convenience to the administrators/deployers, we did not want to force them to enter a 16 byte Master_Key. So we specified the sub-key routine that could handle a variable length Master_Key, one that might be less than 16 bytes. This does NOT mean that administrators are safe to use weak keys. Administrators are encouraged to follow [\[RFC4086\]](#) as listed above. We simply attempted to "put a fence around stupidity", in as much as possible.

This document concerns itself with the selection of cryptographic algorithms for the use of TCP-A0. The algorithms identified in this document as "MUST implement" or "SHOULD implement" are not known to be broken at the current time, and cryptographic research so far leads us to believe that they will likely remain secure into the foreseeable future. Some of the algorithms may be found in the future to have properties significantly weaker than those that were believed at the time this document was produced. Expect that new revisions of this document will be issued from time to time. Be sure to search for more recent versions of this document before implementing.

7. IANA Considerations

IANA has created and will maintain a registry called, "Cryptographic Algorithms for TCP-A0". The registry consists of a text string and an RFC number that lists the associated transform(s). New entries can be added to the registry only after RFC publication and approval by an expert designated by the IESG.

The registry has the following initial values:

SHA1 [This RFC when published]

Internet-Draft

Crypto for TCP-A0

February 2010

AES128

[This RFC when published]

8. Acknowledgements

Eric "EKR" Rescorla, who provided a ton of input and feedback, including a somewhat heavy re-write of [section 3.1.x](#), earning him and author slot on the document.

Paul Hoffman, from whose [\[RFC4308\]](#) I sometimes copied, to quickly create a first draft here.

Tim Polk, whose email summarizing SAAG's guidance to TCPM on the two hash algorithms for TCP-A0 is largely cut and pasted into various sections of this document.

Jeff Schiller, Donald Eastlake and the IPsec WG, whose [\[RFC4307\]](#) & [\[RFC4305\]](#) text was consulted and sometimes used in the Requirements [Section 2](#) section of this document.

(In other words, I was truly only an editor of others' text in creating this document.)

Eric "EKR" Rescorla and Brian Weis, who brought to clarity the issues with the inputs to PRFs for the KDFs. EKR was also of great assistance in how to structure the text, as well as helping to guide good cryptographic decisions.

The TCPM working group, who put up with all us crypto and routing folks DoS'ing their WG for 2 years, and who provided reviews of this document.

9. References

9.1. Normative References

[I-D.ietf-tcpm-tcp-auth-opt]

Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", [draft-ietf-tcpm-tcp-auth-opt-10](#) (work in progress), January 2010.

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

[9.2](#). Informative References

[HMAC-ATTACK]

"On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1", 2006,
<<http://eprint.iacr.org/2006/187>
<http://www.springerlink.com/content/00w4v62651001303>>.

[I-D.narten-iana-considerations-rfc2434bis]

Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs",
[draft-narten-iana-considerations-rfc2434bis-09](#) (work in progress), March 2008.

[NIST-SP800-108]

National Institute of Standards and Technology,
"Recommendation for Key Derivation Using Pseudorandom Functions", SP 800-108, April 2008.

[NIST-SP800-38B]

National Institute of Standards and Technology,
"Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", SP 800-38B, May 2005.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", [RFC 2104](#), February 1997.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within

ESP and AH", [RFC 2404](#), November 1998.

- [RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.
- [RFC4086] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", [BCP 106](#), [RFC 4086](#), June 2005.
- [RFC4305] Eastlake, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", [RFC 4305](#), December 2005.
- [RFC4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", [RFC 4307](#), December 2005.

Lebovitz & Rescorla

Expires August 14, 2010

[Page 18]

Internet-Draft

Crypto for TCP-AO

February 2010

- [RFC4308] Hoffman, P., "Cryptographic Suites for IPsec", [RFC 4308](#), December 2005.
- [RFC4493] Song, JH., Poovendran, R., Lee, J., and T. Iwata, "The AES-CMAC Algorithm", [RFC 4493](#), June 2006.
- [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](#), August 2006.

Authors' Addresses

Gregory Lebovitz
Juniper Networks, Inc.
1194 North Mathilda Ave.
Sunnyvale, CA 94089-1206
US

Phone:

Email: gregory.ietf@gmail.com

Eric Rescorla
RTFM, Inc.
2064 Edgewood Drive
Palo Alto, CA 94303
US

Phone: 650-678-2350
Email: ekr@rtfm.com