

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: October 31, 2008

E. Rescorla  
RTFM, Inc.  
April 29, 2008

TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter  
Mode

[draft-ietf-tls-ecc-new-mac-06.txt](#)

#### Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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/ietf/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 October 31, 2008.

#### Copyright Notice

Copyright (C) The IETF Trust (2008).

#### Abstract

[RFC 4492](#) describes elliptic curve cipher suites for Transport Layer Security (TLS). However, all those cipher suites use SHA-1 as their MAC algorithm. This document describes sixteen new CipherSuites for TLS/DTLS which specify stronger digest algorithms. Eight use HMAC with SHA-256 or SHA-384 and eight use AES in Galois Counter Mode (GCM).

Internet-Draft

TLS ECC New MAC

April 2008

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">1.1.</a>	Conventions Used In This Document . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Cipher Suites . . . . .	<a href="#">3</a>
<a href="#">2.1.</a>	HMAC-based Cipher Suites . . . . .	<a href="#">3</a>
<a href="#">2.2.</a>	Galois Counter Mode-based Cipher Suites . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">4.</a>	IANA Considerations . . . . .	<a href="#">5</a>
<a href="#">5.</a>	Acknowledgements . . . . .	<a href="#">5</a>
<a href="#">6.</a>	References . . . . .	<a href="#">5</a>
<a href="#">6.1.</a>	Normative References . . . . .	<a href="#">5</a>
<a href="#">6.2.</a>	Informative References . . . . .	<a href="#">6</a>
	Author's Address . . . . .	<a href="#">6</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">7</a>

## 1. Introduction

[RFC 4492](#) [[RFC4492](#)] describes Elliptic Curve Cryptography (ECC) cipher suites for Transport Layer Security (TLS). However, all of the [RFC 4492](#) suites use HMAC-SHA1 as their MAC algorithm. Due to recent analytic work on SHA-1 [[Wang05](#)], the IETF is gradually moving away from SHA-1 and towards stronger hash algorithms. This document specifies TLS ECC cipher suites which use SHA-256 and SHA-384 rather than SHA-1.

TLS 1.2 [[I-D.ietf-tls-rfc4346-bis](#)], adds support for authenticated encryption with additional data (AEAD) cipher modes [[RFC5116](#)]. This document also specifies a set of ECC cipher suites using one such mode, Galois Counter Mode (GCM) [[GCM](#)]. Another document [[I-D.ietf-tls-rsa-aes-gcm](#)], provides support for GCM with other key establishment methods.

### 1.1. Conventions Used In This Document

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](#)].

## 2. Cipher Suites

This document defines 8 new cipher suites to be added to TLS. All use Elliptic Curve Cryptography for key exchange and digital signature, as defined in [RFC 4492](#).

### 2.1. HMAC-based Cipher Suites

The first eight cipher suites use AES [[AES](#)] in CBC [[CBC](#)] mode with an HMAC-based MAC:

```
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 = {0xXX,XX};
```

```

CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 = {0xXX,XX};

```

These eight cipher suites are the same as the corresponding cipher suites in [RFC 4492](#) (with names ending in "\_SHA" in place of "\_SHA256" or "\_SHA384"), except for the hash and PRF algorithms, which use SHA-256 and SHA-384 [[SHS](#)] as follows.

Cipher Suite	MAC	PRF
-----	---	---
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA384

## [2.2.](#) Galois Counter Mode-based Cipher Suites

The second eight cipher suites use the same asymmetric algorithms as those in the previous section but use the new authenticated encryption modes defined in TLS 1.2 with AES in Galois Counter Mode (GCM) [[GCM](#)]:

```

CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 = {0xXX,XX};
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 = {0xXX,XX};

```

These cipher suites use authenticated encryption with additional data algorithms AEAD\_AES\_128\_GCM and AEAD\_AES\_256\_GCM described in

[RFC5116]. GCM is used as described in [[I-D.ietf-tls-rsa-aes-gcm](#)].

Cipher Suite	PRF
-----	---
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	P_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	P_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	P_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	P_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	P_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	P_SHA384
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	P_SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	P_SHA384

### 3. Security Considerations

The security considerations in [RFC 4346](#), [RFC 4492](#), and [[I-D.ietf-tls-rsa-aes-gcm](#)] apply to this document as well. In

Rescorla

Expires October 31, 2008

[Page 4]

---

Internet-Draft

TLS ECC New MAC

April 2008

addition, as described in [[I-D.ietf-tls-rsa-aes-gcm](#)], these cipher suites may only be used with TLS 1.2 or greater.

### 4. IANA Considerations

IANA has assigned the following values for these cipher suites:

CipherSuite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	= {0xXX,XX};
CipherSuite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	= {0xXX,XX};
CipherSuite	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	= {0xXX,XX};
CipherSuite	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	= {0xXX,XX};
CipherSuite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	= {0xXX,XX};
CipherSuite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	= {0xXX,XX};
CipherSuite	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	= {0xXX,XX};
CipherSuite	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	= {0xXX,XX};
CipherSuite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	= {0xXX,XX};
CipherSuite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	= {0xXX,XX};
CipherSuite	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	= {0xXX,XX};
CipherSuite	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	= {0xXX,XX};
CipherSuite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	= {0xXX,XX};
CipherSuite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	= {0xXX,XX};

CipherSuite TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256 = {0xXX,XX};  
CipherSuite TLS\_ECDH\_RSA\_WITH\_AES\_256\_GCM\_SHA384 = {0xXX,XX};

## 5. Acknowledgements

This work was supported by the US Department of Defense.

David McGrew contributed substantial sections of the GCM nonce text as well as providing a review of this document.

## 6. References

### 6.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", [RFC 4492](#), May 2006.
- [RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", [RFC 5116](#), January 2008.

- [I-D.ietf-tls-rfc4346-bis] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [draft-ietf-tls-rfc4346-bis-10](#) (work in progress), March 2008.
- [AES] National Institute of Standards and Technology, "Specification for the Advanced Encryption Standard (AES)", FIPS 197, November 2001.
- [SHS] National Institute of Standards and Technology, "Secure Hash Standard", FIPS 180-2, August 2002.
- [CBC] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation - Methods and Techniques", SP 800-38A, December 2001.

[GCM] National Institute of Standards and Technology,  
"Recommendation for Block Cipher Modes of Operation:  
Galois;/Counter Mode (GCM) for Confidentiality and  
Authentication", SP 800-38D, November 2007.

## [6.2.](#) Informative References

[Wang05] Wang, X., Yin, Y., and H. Yu, "Finding Collisions in the  
Full SHA-1", CRYPTO 2005, August 2005.

[I-D.ietf-tls-rsa-aes-gcm]  
Salowey, J., Choudhury, A., and D. McGrew, "AES-GCM Cipher  
Suites for TLS", [draft-ietf-tls-rsa-aes-gcm-03](#) (work in  
progress), April 2008.

## Author's Address

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

Email: [ekr@rtfm.com](mailto:ekr@rtfm.com)

## Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions  
contained in [BCP 78](#), and except as set forth therein, the authors  
retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).