

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: October 25, 2007

M. Salter  
National Security Agency  
E. Rescorla  
Network Resonance  
April 23, 2007

Suite B Cipher Suites for TLS  
draft-ietf-tls-suiteb-00.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/1id-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 25, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

The United States Government has published guidelines for "NSA Suite B Cryptography" dated July, 2005, which defines cryptographic algorithm policy for national security applications. This document defines a profile of TLS which is conformant with Suite B.

Internet-Draft

Suite B for TLS

April 2007

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Conventions Used In This Document . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Suite B Requirements . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Suite B Compliance Requirements . . . . .	<a href="#">4</a>
<a href="#">4.1.</a>	Security Levels . . . . .	<a href="#">4</a>
<a href="#">4.2.</a>	Acceptable Curves . . . . .	<a href="#">5</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">5</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">7.</a>	Acknowledgements . . . . .	<a href="#">6</a>
<a href="#">8.</a>	References . . . . .	<a href="#">6</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">6</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">6</a>
	Authors' Addresses . . . . .	<a href="#">6</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">8</a>

Internet-Draft

Suite B for TLS

April 2007

## 1. Introduction

In July, 2005 the National Security Agency posted "Fact Sheet, NSA Suite B Cryptography" which stated:

To complement the existing policy for the use of the Advanced Encryption Standard (AES) to protect national security systems and information as specified in The National Policy on the use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information (CNSSP-15), the National Security Agency (NSA) announced Suite B Cryptography at the 2005 RSA Conference. In addition to the AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange.

Suite B only specifies the cryptographic algorithms to be used. Many other factors need to be addressed in determining whether a particular device implementing a particular set of cryptographic algorithms should be used to satisfy a particular requirement.

Among those factors are "requirements for interoperability both domestically and internationally".

This document is a profile of of TLS 1.2 [[I-D.ietf-tls-rfc4346-bis](#)] and of the cipher suites defined in [[I-D.ietf-tls-ecc-new-mac](#)], but does not itself define any new cipher suites. This profile requires TLS 1.2.

## 2. 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](#)].

### [3.](#) Suite B Requirements

The "Suite B Fact Sheet" requires that key establishment and authentication algorithms be based on Elliptic Curve Cryptography, that the encryption algorithm be AES [[AES](#)], and that the function used for key derivation and data integrity be SHA [[SHS](#)]. It defines two security levels, of 128 and 192 bits.

In particular it states:

Salter & Rescorla Expires October 25, 2007 [Page 3]

---

Internet-Draft Suite B for TLS April 2007

SUITE B includes:

Encryption:	Advanced Encryption Standard (AES) - FIPS 197 (with keys sizes of 128 and 256 bits)
Digital Signature:	Elliptic Curve Digital Signature Algorithm - FIPS 186-2 (using the curves with 256 and 384-bit prime moduli)
Key Exchange:	Elliptic Curve Diffie-Hellman or Elliptic Curve MQV Draft NIST Special Publication 800-56 (using the curves with 256 and 384-bit prime moduli)
Hashing:	Secure Hash Algorithm - FIPS 180-2 (using SHA-256 and SHA-384)

All implementations of Suite B must, at a minimum, include AES with 128-bit keys, the 256-bit prime modulus elliptic curve and SHA-256 as a common mode for widespread interoperability.

The 128-bit security level corresponds to an elliptic curve size of 256 bits, AES-128, and SHA-256. The 192-bit security level corresponds to an elliptic curve size of 384 bits, AES-256, and SHA-384.

### [4.](#) Suite B Compliance Requirements

To be considered "Suite B compatible" at least one of the Galois Counter Mode (GCM) CipherSuites defined in [[I-D.ietf-tls-ecc-new-mac](#)] MUST be negotiated. In compliance with the guidance in the Suite B Fact Sheet every TLS implementation of Suite B SHOULD implement TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256.

#### [4.1.](#) Security Levels

As described in [Section 1](#), Suite B specifies two security levels, 128 and 192 bit. The following table lists the security levels for each cipher suite:

Salter & Rescorla Expires October 25, 2007 [Page 4]

---

Internet-Draft Suite B for TLS April 2007

Cipher Suite	Security Level
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	192
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	192

#### [4.2.](#) Acceptable Curves

[RFC 4492](#) defines a variety of elliptic curves. For cipher suites defined in this specification, only secp256r1 (23) or secp384r1 (24) may be used. (These are the same curves that appear in FIPS 186-2 as P-256 and P-384, respectively.) For cipher suites at the 128-bit security level, secp256r1 MUST be used. For cipher suites at the 192-bit security level, secp384r1 MUST be used. [RFC 4492](#) requires that uncompressed (0) form be supported. ansiX962\_compressed\_prime(1) point formats MAY be supported.

Clients desiring to negotiate only a Suite B-compliant connection MUST generate a "Supported Elliptic Curves Extension" containing only

the allowed curves. These curves MUST match the cipher suite security levels being offered. Clients which are willing to do both Suite B-compliant and non-Suite B-compliant connections MAY omit the extension or send the extension but offer other curves as well as the appropriate Suite B ones.

Servers desiring to negotiate a Suite B-compliant connection SHOULD check for the presence of the extension, but MUST NOT negotiate inappropriate curves even if they are offered by the client. This allows a Client which is willing to do either Suite B-compliant or non-Suite B-compliant modes to interoperate with a server which will only do Suite B-compliant modes. If the client does not advertise an acceptable curve, the server MUST generate a fatal "handshake\_failure" alert and terminate the connection. Clients MUST check the chosen curve to make sure it is acceptable.

## [5.](#) Security Considerations

Most of the security considerations for this document are described in TLS 1.2 [[I-D.ietf-tls-rfc4346-bis](#)], [RFC 4492](#) [[RFC4492](#)], and [[I-D.ietf-tls-ecc-new-mac](#)]. Readers should consult those documents.

In order to meet the goal of a consistent security level for the entire cipher suite, in Suite B mode TLS implementations MUST ONLY use the curves defined in [Section 4.2](#). Otherwise, it is possible to

have a set of symmetrical algorithms with much weaker or stronger security properties than the asymmetric (ECC) algorithms.

## [6.](#) IANA Considerations

This document defines no actions for IANA.

## [7.](#) Acknowledgements

This work was supported by the US Department of Defense.

## [8.](#) References

## [8.1.](#) 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.
- [I-D.ietf-tls-rfc4346-bis]  
Dierks, T. and E. Rescorla, "The TLS Protocol Version 1.2", [draft-ietf-tls-rfc4346-bis-03](#) (work in progress), March 2007.
- [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.
- [I-D.ietf-tls-ecc-new-mac]  
Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode", April 2007.

## [8.2.](#) Informative References

Salter & Rescorla	Expires October 25, 2007	[Page 6]
-------------------	--------------------------	----------

---

Internet-Draft	Suite B for TLS	April 2007
----------------	-----------------	------------

### Authors' Addresses

Margaret Salter  
National Security Agency  
9800 Savage Rd.  
Fort Meade 20755-6709  
USA

Email: msalter@restarea.ncsc.mil

Eric Rescorla  
Network Resonance  
2483 E. Bayshore #212  
Palo Alto 94303  
USA

Email: ekr@networkresonance.com



Copyright (C) The IETF Trust (2007).

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).