             Suite B Profile for Transport Layer Security (TLS)

Abstract

   The United States government has published guidelines for "NSA Suite
   B Cryptography" that define cryptographic algorithm policy for
   national security applications. This document defines a profile of
   Transport Layer Security (TLS) version 1.2 that is fully compliant
   with Suite B.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6460.

Table of Contents

1. Introduction

   This document specifies the conventions for using National Security
   Agency (NSA) Suite B Cryptography [SuiteB] with the Transport Layer
   Security (TLS) protocol, and the Datagram Transport Layer Security
   (DTLS) protocol.

   This document does not define any new cipher suites; instead, it
   defines a Suite B compliant profile for use with TLS version 1.2
   [RFC5246], DTLS version 1.2 [RFC6347], and the cipher suites defined
   in [RFC5289]. This profile uses only Suite B algorithms.

RFC 5430 defined an additional transitional profile for use with TLS
versions 1.0 [RFC2246] and 1.1 [RFC4346] or with DTLS version 1.0
[RFC4347] and the cipher suites defined in [RFC4492]. When either
the client or the server does not support TLS version 1.2 and DTLS
version 1.2, the transitional profile can be used to achieve
interoperability that is not Suite B compliant. The description for
the transitional profile appears in Annex A of this document.

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].

   We will use the notation "ECDSA-256" to represent the use of the
   Elliptic Curve Digital Signature Algorithm (ECDSA) with the P-256
   curve and the SHA-256 hash function. Similarly, "ECDSA-384" will
   represent the use of the ECDSA with the P-384 curve and the SHA-384
   hash function.

3. Suite B Requirements

   The Fact Sheet on Suite B Cryptography requires key establishment and
   authentication algorithms based on Elliptic Curve Cryptography and
   encryption using AES [AES]. Suite B algorithms are defined to
   support two minimum levels of security: 128 and 192 bits.

   In particular, Suite B includes the following:

      Encryption: Advanced Encryption Standard (AES) [AES] --
                         FIPS 197 (with key sizes of 128 and 256 bits)

      Digital Signature: Elliptic Curve Digital Signature Algorithm
                         (ECDSA) [DSS] - FIPS 186-3 (using the curves
                         with 256- and 384-bit prime moduli)

      Key Exchange: Elliptic Curve Diffie-Hellman (ECDH) - NIST
                         Special Publication 800-56A [PWKE] (using the
                         curves with 256- and 384-bit prime moduli)

   The two elliptic curves used in Suite B each appear in the literature
   under two different names. For sake of clarity, we list both names
   below:

      Curve   NIST name   [SECG] name

      P-256   nistp256   secp256r1
      P-384   nistp384   secp384r1

The purpose of this document is to specify the requirements for a
Suite B compliant implementation of TLS (hereafter referred to as
"Suite B TLS").

3.1. Minimum Levels of Security (minLOS) for Suite B TLS

Suite B provides two levels of cryptographic security, namely a
128-bit minimum level of security (minLOS_128) and a 192-bit minimum
level of security (minLOS_192). Each level defines a minimum
strength that all cryptographic algorithms must provide.

The following combination of algorithms and key sizes are used in
Suite B TLS:

Suite B Combination 1   Suite B Combination 2
-------------------------------   -------------------------------
AES with 128-bit key in GCM mode   AES with 256-bit key in GCM mode
ECDH using the 256-bit prime   ECDH using the 384-bit prime
   modulus curve P-256 [DSS]   modulus curve P-384 [DSS]
TLS PRF with SHA-256 [SHS]   TLS PRF with SHA-384 [SHS]

Suite B TLS configured at a minimum level of security of 128 bits
MUST use a TLS cipher suite satisfying either SuiteB_Combination_1 in
its entirety or SuiteB_Combination_2 in its entirety.

Suite B TLS configured at a minimum level of security of 192 bits
MUST use a TLS cipher suite satisfying SuiteB_Combination_2 in its
entirety.

The specific Suite B compliant cipher suites for each combination are
listed in Section 4.

For Suite B TLS, ECDH uses the Ephemeral Unified Model Scheme with
cofactor set to 1 (see Section 6.1.2.2 in [PWKE]).

To accommodate backward compatibility, a Suite B TLS client or server
MAY be configured to accept a cipher suite that is not part of Suite
B. However, whenever a Suite B TLS client and a Suite B TLS server
establish a TLS version 1.2 session, Suite B algorithms MUST be
employed.

3.2 Suite B TLS Authentication

   Suite B TLS MUST use ECDSA for digital signatures; authentication
   methods other than ECDSA-256 and ECDSA-384 MUST NOT be used for TLS
   authentication. If a relying party receives a signature based on any
   other authentication method, it MUST return a TLS error and stop the
   TLS handshake.

   A system compliant with the Suite B TLS and configured at a minimum
   level of security of 128 bits MUST use either ECDSA-256 or ECDSA-384
   for client or server authentication. One party can authenticate with
   ECDSA-256 when the other party authenticates with ECDSA-384. This
   flexibility allows interoperation between a client and a server that
   have ECDSA authentication keys of different sizes.

   Clients and servers in a system configured at a minimum level of
   security of 128 bits MUST be able to verify ECDSA-256 signatures and
   SHOULD be able to verify ECDSA-384 signatures unless it is absolutely
   certain that the implementation will never need to verify
   certificates originating from an authority that uses an ECDSA-384
   signing key.

   A system compliant with the Suite B TLS and configured at a minimum
   level of security of 192 bits MUST use ECDSA-384 for client and
   server authentication.

   Clients and servers in a system configured at a minimum level of
   security of 192 bits MUST be able to verify ECDSA-384 signatures.

   In all cases, the client MUST authenticate the server. The server
   MAY authenticate the client, as needed by the specific application.

4. Suite B Compliance and Interoperability Requirements

   TLS versions 1.1 [RFC4346] and earlier do not support Galois/ Counter
   Mode (GCM) cipher suites [RFC5289]. However, TLS version 1.2
   [RFC5246] and later do support GCM. For Suite B TLS, GCM cipher
   suites MUST be used; therefore, a Suite B TLS client MUST implement
   TLS version 1.2 or later.

   A Suite B TLS client configured at a minimum level of security of 128
   bits MUST offer the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or the
   TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite in the
   ClientHello message. The TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
   cipher suite is preferred; if offered, it MUST appear before the
   TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite.

If configured at a minimum level of security of 192 bits, the client
MUST offer the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite
and MUST NOT offer the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 cipher
suite.

One of these two cipher suites MUST be the first (most preferred)
cipher suites in the ClientHello message. A Suite B TLS client that
offers interoperability with servers that are not Suite B compliant
MAY offer additional cipher suites, but any additional cipher suites
MUST appear after the two Suite B compliant cipher suites in the
ClientHello message.

A Suite B TLS server MUST implement TLS version 1.2 or later.

A Suite B TLS server configured at a minimum level of security of 128
bits MUST accept either the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
cipher suite or the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher
suite if it is offered in the ClientHello message, with the
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 cipher suite being preferred.

A Suite B TLS server configured at a minimum level of security of 192
bits MUST accept the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher
suite if it is offered in the ClientHello message.

If the server is not offered either of the Suite B cipher suites, and
interoperability with clients that are not Suite B compliant is
desired, then the Suite B TLS server MAY accept another offered
cipher suite that is considered acceptable by the server
administrator.

4.1. Acceptable Curves

RFC 4492 defines a variety of elliptic curves. Suite B TLS
connections MUST use secp256r1(23) or secp384r1(24). These are the
same curves that appear in FIPS 186-3 [DSS] as P-256 and P-384,
respectively. Secp256r1 MUST be used for the key exchange in all
cipher suites in this specification using AES-128; secp384r1 MUST be
used for the key exchange in all cipher suites in this specification
using AES-256. RFC 4492 requires that the uncompressed(0) form be
supported. The ansiX962_compressed_prime(1) point format MAY also be
supported.

Clients desiring to negotiate only a Suite B TLS connection MUST
generate a "Supported Elliptic Curves Extension" containing only the
allowed curves. Clients operating at a minimum level of security of
128 bits MUST include secp256r1 and SHOULD include secp384r1 in the
extension. Clients operating at a minimum level of security of 192
bits MUST include secp384r1 in the extension. In order to be able to

verify ECDSA signatures, a client and server in a system configured
at a minimum level of security of 128 bits MUST support secp256r1 and
SHOULD support secp384r1 unless it is absolutely certain that the
client and server will never need to use or verify certificates
originating from an authority which uses an ECDSA-384 signing key. A
client and server in a system configured at a minimum level of 192
bits MUST support secp384r1.

TLS connections that offer options that are both compliant and non-
compliant with Suite B MAY omit the extension, or they MAY send the
extension but offer other curves as well as the appropriate Suite B
ones.

Servers desiring to negotiate a Suite B TLS connection SHOULD check
for the presence of the extension, but they MUST NOT select a curve
that is not Suite B even if it is offered by the client. This allows
a client that is willing to do either Suite B or non-Suite B TLS
connections to interoperate with a server that will only do Suite B
TLS. 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
that it is one of the Suite B curves.

4.2. Certificates

Server and client certificates used to establish a Suite B TLS
connection MUST be signed with ECDSA and MUST be compliant with the
"Suite B Certificate and Certificate Revocation List (CRL) Profile",
[RFC5759].

4.3. signature_algorithms Extension

The signature_algorithms extension is defined in Section 7.4.1.4.1 of
TLS version 1.2 [RFC5246]. A Suite B TLS version 1.2 or later client
MUST include the signature_algorithms extension. A Suite B TLS
client configured at a minimum level of security of 128 bits MUST
offer SHA-256 with ECDSA and SHOULD offer ECDSA with SHA-384 in the
signature_algorithms extension unless it is absolutely certain that a
client will never need to use or verify certificates originating from
an authority that uses an ECDSA-384 signing key. A Suite B TLS
client configured at a minimum level of 192 bits MUST offer ECDSA
with SHA-384 in the signature_algorithms extension.

Following the guidance in [RFC5759], Suite B TLS connections MUST
only accept signature algorithms ECDSA with either SHA-256 or SHA-384
for certification path validation. (Note that this is a change from
[RFC5430].)

Other offerings MAY be included to indicate the acceptable signature
algorithms in cipher suites that are offered for interoperability
with servers not compliant with Suite B and to indicate the signature
algorithms that are acceptable for certification path validation in
non-compliant Suite B TLS connections.

4.4. CertificateRequest Message

A Suite B TLS server configured at a minimum level of security of 128
bits MUST include ECDSA with SHA-256 and SHOULD include ECDSA with
SHA-384 in the supported_signature_algorithms field of the
CertificateRequest message unless it is absolutely certain that a
server will never need to verify certificates originating from an
authority that uses an ECDSA-384 signing key. A Suite B TLS server
configured at a minimum level of security of 192 bits MUST include
ECDSA with SHA-384 in the supported_signature_algorithms field.

4.5. CertificateVerify Message

Using the definitions found in Section 3.2, a Suite B TLS client MUST
use ECDSA-256 or ECDSA-384 for the signature in the CertificateVerify
message. A Suite B TLS client configured at a minimum security level
of 128 bits MUST use ECDSA-256 or ECDSA-384. A Suite B TLS client
configured at a minimum security level of 192 bits MUST use
ECDSA-384.

4.6. ServerKeyExchange Message Signature

In the TLS_ECDHE_ECDSA-collection of cipher suites, the server sends
its ephemeral ECDH public key and a specification of the
corresponding curve in the ServerKeyExchange message. These
parameters MUST be signed with ECDSA using the server's private key,
which corresponds to the public key in the server's certificate.

A Suite B TLS server MUST sign the ServerKeyExchange message using
either ECDSA-256 or ECDSA-384. A system configured at a minimum
level of security of 128 bits MUST use either ECDSA-256 or ECDSA-384.
A system configured at a minimum level of security of 192-bits MUST
use ECDSA-384.

5. Security Considerations

Most of the security considerations for this document are described
in "The Transport Layer Security (TLS) Protocol Version 1.2"
[RFC5246], "Elliptic Curve Cryptography (ECC) Cipher Suites for
Transport Layer Security (TLS)" [RFC4492], "AES Galois Counter Mode

(GCM) Cipher Suites for TLS" [RFC5288], and "TLS Elliptic Curve
Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)"
[RFC5289]. Readers should consult those documents.

In order to meet the goal of a consistent security level for the
entire cipher suite, Suite B TLS implementations MUST ONLY use the
curves defined in Section 4.1. Otherwise, it is possible to have a
set of symmetric algorithms with much weaker or stronger security
properties than the asymmetric (ECC) algorithms.

6. Acknowledgments

The authors would like to thank Eric Rescorla for his work on the
original RFC 5430.

This work was supported by the US Department of Defense.

7. References

7.1. Normative References

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

   [DSS]   National Institute of Standards and Technology, "Digital
               Signature Standard", FIPS 186-3, June 2009.

   [PWKE]   National Institute of Standards and Technology,
               "Recommendation for Pair-Wise Key Establishment Schemes
               Using Discrete Logarithm Cryptography (Revised)", NIST
               Special Publication 800-56A, March 2007.

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

   [RFC4347]   Rescorla, E. and N. Modadugu, "Datagram Transport Layer
               Security", RFC 4347, April 2006.

   [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.

   [RFC5246]   Dierks, T. and E. Rescorla, "The Transport Layer Security
               (TLS) Protocol Version 1.2", RFC 5246, August 2008.

   [RFC5289]   Rescorla, E., "TLS Elliptic Curve Cipher Suites with
               SHA-256/384 and AES Galois Counter Mode (GCM)", RFC 5289,
               August 2008.

   [RFC5759]   Solinas, J. and L. Zieglar, "Suite B Certificate and
               Certificate Revocation List (CRL) Profile", RFC 5759,
               January 2010.

   [SHS]   National Institute of Standards and Technology, "Secure
               Hash Standard", FIPS 180-3, October 2008.

   [RFC6347]   Rescorla, E. and N. Modadugu, "Datagram Transport Layer
               Security Version 1.2", RFC 6347, January 2012.

7.2. Informative References

   [RFC2246]   Dierks, T. and C. Allen, "The TLS Protocol Version 1.0",
               RFC 2246, January 1999.

   [RFC4346]   Dierks, T. and E. Rescorla, "The Transport Layer Security
               (TLS) Protocol Version 1.1", RFC 4346, April 2006.

   [RFC5288]   Salowey, J., Choudhury, A., and D. McGrew, "AES Galois
               Counter Mode (GCM) Cipher Suites for TLS", RFC 5288,
               August 2008.

   [RFC5430]   Salter, M., Rescorla, E., and R. Housley, "Suite B Profile
               for Transport Layer Security (TLS)", RFC 5430, March 2009.

   [SECG]   Brown, D., "SEC 2: Recommended Elliptic Curve Domain
               Parameters",
               http://www.secg.org/download/aid-784/sec2-v2.pdf, February
               2010.

   [SuiteB]   National Security Agency, "Fact Sheet NSA Suite B
               Cryptography", November 2010,
               http://www.nsa.gov/ia/programs/suiteb_cryptography/.

Annex A. A Transitional Suite B Profile for TLS 1.1 and 1.0

   A transitional profile is described for use with TLS version 1.0
   [RFC2246], TLS version 1.1 [RFC4346], or DTLS version 1.0 [RFC4347]
   and the cipher suites defined in [RFC4492]. This profile uses the
   Suite B cryptographic algorithms to the greatest extent possible and
   provides backward compatibility. While the transitional profile is
   not a Suite B Compliant implementation of TLS, it provides a
   transitional path towards the Suite B compliant Profile.

   The following combination of algorithms and key sizes are defined for
   use with the Suite B TLS transitional profile:

   Transitional Suite B Combination 1 Transitional Suite B Combination 2
   ---------------------------------- ----------------------------------
   AES with 128-bit key in CBC mode   AES with 256-bit key in CBC mode
   ECDH using the 256-bit prime   ECDH using the 384-bit prime
      modulus curve P-256 [DSS]   modulus curve P-384 [DSS]
   Standard TLS PRF   Standard TLS PRF
      (with SHA-1 and MD5)   (with SHA-1 and MD5)
   HMAC with SHA-1 for message   HMAC with SHA-1 for message
      authentication   authentication

   A Transitional Suite B TLS system configured at a minimum level of
   security of 128 bits MUST use a TLS cipher suite satisfying either
   Transitional Suite B Combination 1 in its entirety or Transitional
   Suite B Combination 2 in its entirety.

   A Transitional Suite B TLS system configured at a minimum level of
   security of 192 bits MUST use a TLS cipher suite satisfying
   Transitional Suite B Combination 2 in its entirety.

   TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA and
   TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA satisfy the requirements of
   Transitional Suite B Combination 1 and Transitional Suite B
   Combination 2, respectively.

   A Transitional Suite B TLS client MUST implement TLS version 1.1 or
   earlier.

   A Transitional Suite B TLS system configured at a minimum level of
   security of 128 bits, MUST offer the
   TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA cipher suite and/or the
   TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA cipher suite in the

ClientHello message. The TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA cipher
suite is preferred; if it is offered, it MUST appear before the
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA cipher suite (if present).

A Transitional Suite B TLS system configured at a minimum level of
security of 192 bits MUST offer the
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA cipher suite in the ClientHello
message.

One of these Transitional Suite B cipher suites MUST be the first
(most preferred) in the ClientHello message.

A Transitional Suite B client that offers interoperability with
servers that are not Suite B transitional MAY offer additional cipher
suites. If any additional cipher suites are offered, they MUST
appear after the Transitional Suite B cipher suites in the
ClientHello message.

A Transitional Suite B TLS server MUST implement TLS version 1.1 or
earlier.

A Transitional Suite B TLS server configured at a minimum level of
security of 128 bits MUST accept the
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA cipher suite (preferred) or the
TLS_ECHDE_ECDSA_WITH_AES_256_CBC_SHA cipher suite if offered in the
ClientHello message.

A Transitional Suite B TLS server configured at a minimum level of
security of 192 bits MUST accept the
TLS_ECHDE_ECDSA_WITH_AES_256_CBC_SHA cipher suite if offered in the
ClientHello message.

If a Transitional Suite B TLS server is not offered the Transitional
Suite B cipher suites and interoperability with non-Transitional
Suite B clients is desired, then the server MAY accept another
offered cipher suite that is considered acceptable by the server
administrator.

A Transitional Suite B TLS server MUST sign the ServerKeyExchange
message using ECDSA with SHA-1. The Transitional Suite B profile
does not impose any additional restrictions on the server certificate
signature or the signature schemes used elsewhere in the
certification path. Likewise, the Transitional Suite B Profile does
not impose restrictions on signature schemes used in the
certification path for the client's certificate when mutual
authentication is employed.

Annex B. Changes since RFC 5430

   The changes from RFC 5430 [RFC5430] are as follows:

     - The transitional profile for use with TLS version 1.0, TLS version
       1.1, and DTLS version 1.0 was moved to an annex.

     - The requirement of Section 4 of RFC 5430 that a Suite B TLS 1.2
       Client offer the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 or
       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 cipher suites was removed.

     - A Suite B TLS system configured at a minimum level of security of
       128 bits MUST use either TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
       or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, with the first being
       preferred.

     - A Suite B TLS system configured at a minimum level of security of
       128 bits MUST use either ECDSA on the secp256r1 curve with SHA-256
       or ECDSA on the secp384r1 curve with SHA-384. One party can
       authenticate with ECDSA on the secp256r1 curve and SHA-256 when
       the other party authenticates with ECDSA on the secp384r1 curve
       and SHA-384.

     - A system desiring to negotiate a Suite B TLS connection at a
       minimum level of security of 128 bits MUST generate a "Supported
       Elliptic Curves Extension", MUST include secp256r1 in the
       extension, and SHOULD include secp384r1 in the extension.

     - A client and server, in order to verify digital signatures in a
       Suite B TLS system configured at a minimum level of security of
       128 bits, MUST support secp256r1 and SHOULD support secp384r1.

     - A Suite B TLS client configured at a minimum level of security of
       128 bits MUST offer SHA-256 with ECDSA and SHOULD offer SHA-384
       with ECDSA in the signature_algorithms extension.

     - Certification path validation MUST only include certificates
       containing an ECDSA public key on the secp256r1 curve or on the
       secp384r1 curve. The ECDSA public keys used in the certification
       path MUST be in non-descending order of size from the end entity
       public key to the root public key.

     - A Suite B TLS server configured at a minimum level of security of
       128 bits MUST include ECDSA with SHA-256 and SHOULD include ECDSA
       with SHA-384 in the supported_signature_algorithms field of the
       CertificateRequest message.

- A Suite B TLS client configured at a minimum level of security of
  128 bits MUST use ECDSA on the secp256r1 curve and SHA-256 or
  ECDSA on the secp384r1 curve and SHA-384.

- A Suite B TLS server configured at a minimum level of security of
  128 bits MUST use either ECDSA on the secp256r1 curve and SHA-256
  or ECDSA on the secp384r1 curve and SHA-384 when signing the
  ServerKeyExchange message.

Authors' Addresses

   Margaret Salter
   National Security Agency
   9800 Savage Rd.
   Fort Meade 20755-6709
   USA
   EMail: misalte@nsa.gov

   Russ Housley
   Vigil Security
   918 Spring Knoll Drive
   Herndon 21070
   USA
   EMail: housley@vigilsec.com