SM3 and SM4 Cipher Suites for TLS
draft-sca-curdle-tls-sm34-00

Abstract

This document describes TLS cipher suites that utilize the SM3 cryptographic hash algorithm (GB/T 32905-2016) and SM4 symmetric blockcipher algorithm (GB/T 32907-2016), both published by the State Cryptography Administration of China (SCA).

This document is a product of the Crypto Forum Research Group (CFRG).

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 October 24, 2018.

Copyright Notice

Copyright (c) 2018 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.
1. Introduction

The SM3 [I-D.sca-cfrg-sm3] [GBT.32905-2016] [ISO.IEC.10118-3] and SM4 [I-D.ribose-cfrg-sm4] [GBT.32907-2016] [ISO.IEC.18033-3.AMD2] algorithms are published by the State Cryptography Administration (SCA) of China [SCA] for authorized use within China. Both algorithms are published in public, and now commonly available in cryptographic libraries.

SM3 is as a cryptographic hash algorithm that produces an output hash value of 256 bits long, based on 512-bit input message blocks, on input lengths up to $2^m$.

SM4 is a symmetric encryption algorithm, a blockcipher to be exact, designed for data encryption that acts on 128-bit blocks.

TLS versions at and beyond 1.2 [RFC5246] contain support for authenticated encryption with additional data (AEAD) cipher modes [RFC5116].

This document describes the use of SM4 [I-D.ribose-cfrg-sm4] in conjunction with various key exchange mechanisms as a cipher suite for TLS, in two ways:

- by using SM4 with authentication encryption modes (CCM, GCM, OCB), in a manner similar to [RFC7251];
o by using SM4 together with SM3 [I-D.sca-cfrg-sm3] as MAC, in a manner similar to [RFC5288], [RFC5289] and [RFC7539].

TODO: describe SM4 AE modes...

2. Terms 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Cipher Suites

Cipher suites defined in this document are based on the SM4-CCM Authenticated Encryption with Associated Data (AEAD) algorithms AEAD_SM4_128_CCM and AEAD_SM4_256_CCM described in [[I-D.ribose-cfrg-sm4ae]].

3.1. HMAC-Based

These cipher suites use SM4 in Cipher Block Chaining (CBC) mode with an HMAC-based MAC:

CipherSuite TLS_ECDHE_ECDSA_WITH_SM4_CBC_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDH_ECDSA_WITH_SM4_CBC_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDH_RSA_WITH_SM4_CBC_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDH_RSA_WITH_SM4_CBC_SM3 = {0xYY,0xYY};

These cipher suites are the same as the corresponding cipher suites in [RFC5289] (with names here ending in "_SM3" inplace of "_SHA256"), except for the MAC and Pseudo Random Function (PRF) algorithms.

The PRF is the TLS PRF [RFC5246] with SM3 as the hash function. The MAC is HMAC [RFC2104] with SM3 as the hash function.

3.2. Galois Counter Mode-Based

These cipher suites use the same asymmetric algorithms as those in the previous section, but use the authenticated encryption modes defined in TLS 1.3 [I-D.ietf-tls-tls13] with SM4 in Galois Counter Mode (GCM):
CipherSuite TLS_ECDHE_ECDSA_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDH_ECDSA_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDHE_RSA_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDH_RSA_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_RSA_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_DHE_RSA_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_DHE_DSS_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_DH_DSS_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_DH_anon_WITH_SM4_GCM_SM3 = {0xYY,0xYY};

These cipher suites use the authenticated encryption with additional data algorithm AEAD_SM4_GCM described in [[I-D.ribose-cfrg-sm4ae]].

Each of these AEAD algorithms uses a 128-bit authentication tag with GCM (in particular, as described in 3.5 [RFC4366] and 3 [RFC5288].

The PRF is the TLS PRF [RFC5246] with SM3 as the hash function.

3.3. Counter and CBC-MAC Mode-Based

These cipher suites use the same asymmetric algorithms as those in the previous section, but use the authenticated encryption modes defined in TLS 1.3 with SM4 in Counter and CBC-MAC Mode (CCM):

CipherSuite TLS_ECDHE_ECDSA_WITH_SM4_CCM = {0xYY,0xYY};
CipherSuite TLS_ECDH_ECDSA_WITH_SM4_CCM = {0xYY,0xYY};
CipherSuite TLS_ECDHE_RSA_WITH_SM4_CCM = {0xYY,0xYY};
CipherSuite TLS_ECDH_RSA_WITH_SM4_CCM = {0xYY,0xYY};
CipherSuite TLS_RSA_WITH_SM4_CCM = {0xYY,0xYY};
CipherSuite TLS_DHE_RSA_WITH_SM4_CCM = {0xYY,0xYY};
CipherSuite TLS_DHE_DSS_WITH_SM4_CCM = {0xYY,0xYY};
CipherSuite TLS_DH_DSS_WITH_SM4_CCM = {0xYY,0xYY};
CipherSuite TLS_DH_anon_WITH_SM4_CCM = {0xYY,0xYY};

These cipher suites use the authenticated encryption with additional data algorithm AEAD_SM4_CCM described in [[I-D.ribose-cfrg-sm4ae]].

Each of these AEAD algorithms uses a 128-bit authentication tag with CCM (in particular, as described in 3.5 [RFC4366] and 3 [RFC5288].

The "nonce" input to the AEAD algorithm is as defined in [RFC6655].

The PRF is the TLS PRF [RFC5246] with SM3 as the hash function.
3.4. OCB

The following cipher suites are defined:

CipherSuite TLS_ECDHE_ECDSA_WITH_SM4_OCB = {0xYY,0xYY}

The "nonce" input to the AEAD algorithm is as defined in [RFC6655].

The PRF is the TLS PRF [RFC5246] with SM3 as the hash function.

Further requirements provided in 2 [RFC7251] apply.

4. TLS Versions

These cipher suites make use of the authenticated encryption with additional data defined in TLS 1.2 [RFC5288].

- They *MUST NOT* be negotiated in older versions of TLS.
- Clients *MUST NOT* offer these cipher suites if they do not offer TLS 1.2 or later.
- Servers that select an earlier version of TLS *MUST NOT* select one of these ciphersuites. Earlier versions do not have support for AEAD; for instance, the TLScipherertext structure does not have the "aead" option in TLS 1.1. Because TLS has no way for the client to indicate that it supports TLS 1.2 but not earlier versions, a non-compliant server might potentially negotiate TLS 1.1 or earlier and select one of the cipher suites in this document.
- Clients *MUST* check the TLS version and generate a fatal "illegal_parameter" alert if they detect an incorrect version.

5. Security Considerations

The security considerations in [RFC4346], [RFC4492], [I-D.ribose-cfrg-sm4], [I-D.sca-cfrg-sm3] apply.

- Products and services that utilize cryptography are regulated by the SCA [SCA]; they must be explicitly approved or certified by the SCA before being allowed to be sold or used in China.
- The cipher suites described in this document *SHOULD** only be used with TLS 1.3 or greater [I-D.ietf-tls-tls13].
CCM security requires that the counter never be reused. The nonce/IV requirement in Section 3.3 is designed to prevent counter reuse.

6. IANA Considerations

IANA has assigned the following values for these cipher suites:

CipherSuite TLS_ECDHE_ECDSA_WITH_SM4_CBC_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDH_ECDSA_WITH_SM4_CBC_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDHE_RSA_WITH_SM4_CBC_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDH_RSA_WITH_SM4_CBC_SM3 = {0xYY,0xYY};
CipherSuite TLS_ECDHE_ECDSA_WITH_SM4_GCM_SM4 = {0xYY,0xYY};
CipherSuite TLS_ECDH_ECDSA_WITH_SM4_GCM_SM4 = {0xYY,0xYY};
CipherSuite TLS_ECDHE_RSA_WITH_SM4_GCM_SM4 = {0xYY,0xYY};
CipherSuite TLS_ECDH_RSA_WITH_SM4_GCM_SM4 = {0xYY,0xYY};
CipherSuite TLS_RSA_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_DHE_RSA_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_DH_RSA_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_DHE_DSS_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_DH_DSS_WITH_SM4_GCM_SM3 = {0xYY,0xYY};
CipherSuite TLS_DH_anon_WITH_SM4_GCM_SM3 = {0xYY,0xYY};

7. References

7.1. Normative References

[GBT.32905-2016]
Standardization Administration of the People’s Republic of China, "GB/T 32905-2016: Information security techniques -- SM3 cryptographic hash algorithm", August 2016,

[GBT.32907-2016]
Standardization Administration of the People’s Republic of China, "GB/T 32907-2016: Information security technology -- SM4 block cipher algorithm", August 2016,

[I-D.ietf-tls-tls13]
[I-D.ribose-cfrg-sm4]

[I-D.ribose-cfrg-sm4ae]
Tse, R., Wong, W., and M. Saarinen, "Authenticated Encryption For The SM4 Blockcipher Algorithm", draft-ribose-cfrg-sm4ae-00 (work in progress), April 2018.

[I-D.sca-cfrg-sm3]

[ISO.IEC.10118-3]

[ISO.IEC.18033-3.AMD2]


7.2. Informative References

[GB.15629.11-2003]

[GBT.33560-2017]

[GMT-0002-2012]

[GMT-0004-2012]

[GMT-0006-2012]

[ISO.IEC.18033-3]

[NIST.SP.800-38A]


Appendix A.  Acknowledgements

This document borrows heavily from [RFC5288], [RFC5289], [RFC7251].

Authors’ Addresses

Paul Y. Yang
BaishanCloud
Building 16-3, Baitasan Street
Shenyang, Liaoning 110000
People’s Republic of China

Email: yang.yang@baishancloud.com
URI: https://www.baishancloud.com

Ronald Henry Tse
Ribose
Suite 1111, 1 Pedder Street
Central, Hong Kong
People’s Republic of China

Email: ronald.tse@ribose.com
URI: https://www.ribose.com

Markku-Juhani O. Saarinen
Independent Consultant

Email: mjos@iki.fi
URI: https://mjos.fi/