Workgroup: Network Working Group
Internet-Draft:
draft-corcoran-cnsa-ipsec-profile-06
Published: 11 January 2022
Intended Status: Informational
Expires: 15 July 2022

Authors: L. Corcoran   M. Jenkins
NSA   NSA

Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec)

Abstract

The United States Government has published the National Security Agency's Commercial National Security Algorithm (CNSA) Suite, which defines cryptographic algorithm policy for national security applications. This document specifies the conventions for using the United States National Security Agency's CNSA Suite algorithms in Internet Protocol Security. It applies to the capabilities, configuration, and operation of all components of US National Security Systems that employ IPsec. US National Security Systems are described in NIST Special Publication 800-59. It is also appropriate for all other US Government systems that process high-value information. It is made publicly available for use by developers and operators of these and any other system deployments.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document specifies conventions for using the United States National Security Agency's Commercial National Security Algorithm (CNSA) Suite algorithms [CNSA] in Internet Protocol Security (IPsec). It defines CNSA-based user interface suites ("UI suites") describing sets of security configurations for Internet Key Exchange version 2 (IKEv2) and IP Encapsulating Security Payload (ESP) protocol use, and specifies certain other constraints with respect to algorithm selection and configuration. It applies to the capabilities, configuration, and operation of all components of US National Security Systems that employ IPsec. US National Security Systems are described in NIST Special Publication 800-59 [SP80059]. It is also appropriate for all other US Government systems that process high-value information. It is made publicly available for use by developers and operators of these and any other system deployments.

The reader is assumed to have familiarity with the following:

[RFC4303], IP Encapsulating Security Payload (ESP)

[RFC5280], Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC7296], Internet Key Exchange Version 2 (IKEv2)

[RFC8221], Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)

[RFC8603], Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile

2. Terminology

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.

AES refers to the Advanced Encryption Standard. ECDSA and ECDH refer to the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH), respectively. DH refers to Diffie-Hellman key establishment. RSA refers to RSA signature.

3. The Commercial National Security Algorithm Suite

The National Security Agency (NSA) profiles commercial cryptographic algorithms and protocols as part of its mission to support secure, interoperable communications for US Government National Security Systems. To this end, it publishes guidance both to assist with the US Government transition to new algorithms, and to provide vendors - and the Internet community in general - with information concerning their proper use and configuration.

Recently, cryptographic transition plans have become overshadowed by the prospect of the development of a cryptographically-relevant quantum computer. NSA has established the Commercial National Security Algorithm (CNSA) Suite to provide vendors and IT users near-term flexibility in meeting their information assurance interoperability requirements. The purpose behind this flexibility is to avoid vendors and customers making two major transitions in a relatively short timeframe, as we anticipate a need to shift to quantum-resistant cryptography in the near future.

NSA is authoring a set of RFCs, including this one, to provide updated guidance concerning the use of certain commonly available commercial algorithms in IETF protocols. These RFCs can be used in conjunction with other RFCs and cryptographic guidance (e.g., NIST Special Publications) to properly protect Internet traffic and data-at-rest for US Government National Security Systems.

4. CNSA Compliant IPsec Overview

CNSA compliant implementations for IPsec MUST use IKEv2 [RFC7296].

Implementing a CNSA compliant IPsec system requires cryptographic algorithm selection for both the IKEv2 and ESP protocols. The following CNSA requirements apply to IPsec:

Encryption:

AES [FIPS197] (with key size 256 bits)

Digital Signature:

ECDSA [FIPS186] (using the NIST P-384 elliptic curve)

RSA [FIPS186] (with a modulus of 3072 bits or larger)

Key Establishment:

ECDH [SP80056A] (using the NIST P-384 elliptic curve)

DH [RFC3526] (with a prime modulus of 3072 or larger)

To facilitate selection of appropriate combinations of compliant algorithms, this document provides CNSA compliant user interface suites (UI Suites) [RFC4308] to implement IPsec on NSS.

The approved CNSA hash function for all purposes is SHA-384, as defined in [FIPS180]. However, PRF_HMAC_SHA-512 is specified for the IKEv2 PRF instead of PRF_HMAC_SHA-384 due to availability. See Section 8 below.

For CNSA Suite applications, public key certificates MUST be compliant with the CNSA Suite Certificate and CRL Profile specified in [RFC8603].

Under certain conditions, such as applications having long-lived data protection requirements, systems that do not comply with the requirements of this document are acceptable; see Section 12.

5. IPsec User Interface Suites

User Interface (UI) suites [RFC4308] are named suites that cover some typical security policy options for IPsec. Use of UI suites does not change the IPsec protocol in any way. The following UI suites provide cryptographic algorithm choices for ESP [RFC4303] and for Internet Key Exchange (IKEv2) [RFC7296]. The selection of a UI Suite will depend on the key exchange algorithm. The suite names indicate the Advanced Encryption Standard [FIPS197] mode, AES key length specified for encryption, and the key exchange algorithm.

Although RSA is also a CNSA approved key establishment algorithm, in IPsec with IKEv2 [RFC7296] only DH or ECDH are implemented for key exchange. RSA in IPsec is used only for digital signatures. See Section 6.

ESP requires negotiation of both a confidentiality algorithm and an integrity algorithm. However, authenticated encryption (AEAD) algorithms [RFC5116] do not require a separate integrity algorithm to be negotiated. In particular, since AES-GCM is an AEAD algorithm, ESP implementing AES-GCM MUST either offer no integrity algorithm, or indicate the single integrity algorithm NONE (see Section 3.3 of [RFC7296]).

To be CNSA compliant, IPsec implementations that use the following UI suites MUST use the suite names listed below. IPsec implementations SHOULD NOT use names different than those listed here for the suites that are described, and MUST NOT use the names listed here for suites that do not match these values. These requirements are necessary for interoperability.

Transform names are as listed in the IANA registry for Internet Key Exchange Version 2 (IKEv2) Parameters. Definitions of the transforms are contained in the references specified in that registry.

Other UI suites may be acceptable for CNSA compliance. See Section 8 for details.

5.1. Suite CNSA-GCM-256-ECDH-384

```
ESP SA:

   Encryption: ENCR_AES_GCM_16 (with key size 256 bits)
   Integrity: NONE
IKEv2 SA:

   Encryption: ENCR_AES_GCM_16 (with key size 256 bits)
   PRF: PRF_HMAC_SHA2_512
   Integrity: NONE
   Diffie-Hellman group: 384-bit random ECP group
```

5.2. Suite CNSA-GCM-256-DH-3072

ESP SA:

Encryption: ENCR_AES_GCM_16 (with key size 256 bits)
Integrity: NONE

IKEv2 SA:

Encryption: ENCR_AES_GCM_16 (with key size 256 bits)
PRF: PRF_HMAC_SHA2_512
Integrity: NONE
Diffie-Hellman group: 3072-bit MODP Group

5.3. Suite CNSA-GCM-256-DH-4096

ESP SA:

Encryption: ENCR_AES_GCM_16 (with key size 256 bits)
Integrity: NONE

IKEv2 SA:

Encryption: ENCR_AES_GCM_16 (with key size 256 bits)
PRF: PRF_HMAC_SHA2_512
Integrity: NONE
Diffie-Hellman group: 4096-bit MODP Group

6. IKEv2 Authentication

Authentication of the IKEv2 Security Association (SA) requires computation of a digital signature. To be CNSA compliant, digital signatures MUST be generated with either ECDSA-384 as defined in [RFC4754] or RSA with 3072-bit or greater modulus and SHA-384 as defined in [RFC8017]. (For applications with long data-protection requirements, somewhat different rules apply; see Section 12.)

Initiators and responders MUST be able to verify ECDSA-384 signatures and MUST be able to verify RSA with 3072-bit or 4096-bit modulus and SHA-384 signatures.

For CNSA compliant systems, authentication methods other than ECDSA-384 or RSA MUST NOT be accepted for IKEv2 authentication. A 3072-bit modulus or larger MUST be used for RSA. If the relying party receives a message signed with any authentication method other than ECDSA-384 or RSA signature it MUST return an AUTHENTICATION_FAILED notification and stop processing the message. If the relying party receives a message signed with RSA using less than a 3072-bit modulus, it MUST return an AUTHENTICATION_FAILED notification and stop processing the message.

7. Certificates

To be CNSA compliant, the initiator and responder MUST use X.509 certificates that comply with [RFC8603]. Peer authentication decisions must be based on the Subject or Subject Alternative Name from the certificate that contains the key used to validate the signature in the Authentication Payload defined in Section 3.8 of [RFC7296], rather than the Identification Data from the Identification Payload that is used to look up policy.

8. IKEv2 Security Associations (SA)

Section 5 specifies three UI suites for ESP and IKEv2 Security Associations. All three use AES-GCM for encryption but differ in the key exchange algorithm. Galois Counter Mode (GCM) [RFC4106] combines counter (CTR) mode with a secure, parallelizable, and efficient authentication mechanism. Since AES-GCM is an AEAD algorithm, ESP implements AES-GCM with no additional integrity algorithm (see Section 3.3 of [RFC7296]).

An initiator proposal SHOULD be constructed from one or more of the following suites:

CNSA-GCM-256-ECDH-384,
CNSA-GCM-256-DH-3072,
CNSA-GCM-256-DH-4096.

A responder SHOULD accept proposals constructed from at least one of the three named suites. Other UI suites may result in acceptable proposals (such as those based on PRF_HMAC_SHA2_384); however, these are provided to promote interoperability.

Nonce construction for AES-GCM using a misuse-resistant technique [RFC8452] conforms with the requirements of this document and MAY be used if a Federal Information Processing Standard (FIPS) validated implementation is available.

The named UI suites specify PRF_HMAC_SHA2_512 for the IKEv2 SA PRF transform as PRF_HMAC_SHA2_384 is not listed among required PRF transforms in [RFC8247]; therefore, implementation of the latter is likely to be scarce. The security level of PRF_HMAC_SHA2_512 is comparable, and the difference in performance is negligible. However, SHA-384 is the official CNSA algorithm for computing a condensed representation of information. Therefore, the PRF_HMAC_SHA2_384 transform is CNSA compliant if it is available to initiator and responder. Any PRF transform other than PRF_HMAC_SHA2_384 or PRF_HMAC_SHA2_512 MUST NOT be used.

If none of the proposals offered by the initiator consist solely of transforms based on CNSA algorithms (such as those in the UI Suites defined in Section 5, the responder MUST return a Notify payload with the error NO_PROPOSAL_CHOSEN when operating in CNSA compliant mode.

9. The Key Exchange Payload in the IKE_SA_INIT Exchange

The key exchange payload is used to exchange Diffie-Hellman public numbers as part of a Diffie-Hellman key exchange. The CNSA compliant initiator and responder MUST each generate an ephemeral key pair to be used in the key exchange.

If the Elliptic Curve Diffie-Hellman (ECDH) key exchange is selected for the SA, the initiator and responder both MUST generate an elliptic curve (EC) key pair using the P-384 elliptic curve. The ephemeral public keys MUST be stored in the key exchange payload as in [RFC7296].

If the Diffie-Hellman (DH) key exchange is selected for the SA, the initiator and responder both MUST generate a key pair using the appropriately sized MODP group as described in [RFC3526]. The size of the MODP group will be determined by the selection of either a 3072-bit or greater modulus for the SA.

10. Generating Key Material for the IKE SA

As noted in Section 7 of [RFC5903], the shared secret result of a ECDH key exchange is the 384 bit x value of the ECDH common value. The shared secret result of a DH key exchange is the number of octets needed to accomodate the prime (e.g. 384 octets for 3072 MODP) with leading zeros as necessary, as described in Section 2.1.2 of [RFC2631].

IKEv2, Section 2.12 [RFC7296] allows for the reuse of Diffie-Hellman private keys. However, there are security concerns related to this practice. Section 5.6.3.3 of [SP80056A] states that an ephemeral private key MUST be used in exactly one key establishment transaction and MUST be destroyed (zeroized) as soon as possible. Section 5.8 of [SP80056A] states that a Diffie-Hellman shared secret must be destroyed (zeroized) immediately after its use. CNSA compliant IPsec systems MUST follow the mandates in [SP80056A].

11. Additional Requirements

The IPsec protocol AH MUST NOT be used in CNSA compliant implementations.

A Diffie-Hellman group MAY be negotiated for a Child SA as described in Section 1.3 of [RFC7296] allowing peers to employ Diffie-Hellman in the CREATE_CHILD_SA exchange. If a transform of type 4 is specified for an SA for ESP, the value of that transform MUST match the value of the transform used by the IKEv2 SA.

Per [RFC7296], if a CREATE_CHILD_SA exchange includes a KEi payload, at least one of the SA offers MUST include the Diffie-Hellman group of the KEi. For CNSA compliant IPsec compliant implementations, the Diffie-Hellman group of the KEi MUST use the same group used in the IKE_INIT_SA.

For IKEv2, rekeying of the CREATE_CHILD_SA MUST be supported by both parties. The initiator of this exchange MAY include a new Diffie-Hellman key; if it is included, it MUST use the same group used in the IKE_INIT_SA. If the initiator of the exchange includes a Diffie-Hellman key, the responder MUST include a Diffie-Hellman key, and it MUST use the same group.

For CNSA compliant systems, the IKEv2 authentication method MUST use an end-entity certificate provided by the authenticating party. Identification Payloads (Idi and IDr) in the IKE_AUTH exchanges MUST NOT be used for the IKEv2 authentication method , but may be used for policy lookup.

The administrative user interface (UI) for a system that conforms to this profile MUST allow the operator to specify a single suite. If only one suite is specified in the administrative UI, the IKEv2 implementation MUST only offer algorithms for that one suite.

The administrative UI MAY allow the operator to specify more than one suite; if it allows this, it MUST allow the operator to specify a preferred order for the suites that are to be offered or accepted. If more than one suite is specified in the administrative UI, the IKEv2 implementation MUST only offer algorithms of those suites. (Note that although this document does not define a UI suite specifying PRF_HMAC_SHA2_384, a proposal containing such a transform is CNSA compliant.)

12. Guidance for Applications With Long Data-Protection Requirements

The CNSA mandate is to continue to use current algorithms with increased security parameters, then transition to approved post-quantum resilient algorithms when they are identified. However, some applications have data-in-transit-protection requirements that are long enough that post-quantum resilient protection must be provided now. Lacking approved asymmetric post-quantum resilient confidentiality algorithms, that means approved symmetric techniques must be used as described in this section until approved post-quantum resilient asymmetric algorithms are identified.

For new applications, confidentiality and integrity requirements from the sections above MUST be followed, with the addition of a PSK mixed in as defined in [RFC8784].

Installations currently using IKEv1 with PSK MUST use AES in cipher block chaining mode (AES-CBC) in conjunction with a CNSA compliant integrity algorithm (e.g. AUTH_HMAC_SHA2_384_192), and transition to IKEv2 with PSK [RFC8784] as soon as implementations become available.

Specific guidance for systems not compliant with the requirements of this document, including non-GCM modes and PSK length and randomness, will be defined in solution specific requirements appropriate to the application. Details of those requirements will depend on the program under which the commercial NSS solution is developed (e.g. Commercial Solutions for Classified Capability Package).

13. Security Considerations

This document inherits all of the security considerations of the IPsec and IKEv2 documents, including [RFC7296], [RFC4303], [RFC4754], and [RFC8221].

The security of a system that uses cryptography 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 and administration of the protocol used by the system to ensure that there are no non-cryptographic ways to bypass the security of the overall system.

When selecting a mode for the AES encryption [RFC5116] , be aware that nonce reuse can result in a loss of confidentiality. Nonce reuse is catastrophic for GCM since it also results in a loss of integrity.

14. IANA Considerations

IANA is asked to amend the registry titled "Cryptographic Suites for IKEv1, IKEv2, and IPsec" located at https://www.iana.org/assignments/crypto-suites as described in this section. The registry consists of a text string and an RFC number that lists the associated transforms. The UI suites defined in this document are listed, with this document as the RFC reference.

Identifier	Reference
CNSA-GCM-256-ECDH-384	[this document when published]
CNSA-GCM-256-DH-3072	[this document when published]
CNSA-GCM-256-DH-4096	[this document when published]

Table 1

15. References

15.1. Normative References

[CNSA] Committee for National Security Systems, "Use of Public Standards for Secure Information Sharing", CNSSP 15, October 2016, <https://www.cnss.gov/CNSS/Issuances/Policies.htm>.

[FIPS180] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", Federal Information Processing Standard 180-4, August 2015, <https://csrc.nist.gov/publications/detail/fips/180/4/final>.

[FIPS186] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", NIST Federal Information Processing Standard 186-4, July 2013, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>.

[FIPS197] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", Federal Information Processing Standard 197, November 2001, <https://csrc.nist.gov/publications/detail/fips/197/final>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2631] Rescorla, E., "Diffie-Hellman Key Agreement Method", RFC 2631, DOI 10.17487/RFC2631, June 1999, <https://www.rfc-editor.org/info/rfc2631>.

[RFC3526] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, DOI 10.17487/RFC3526, May 2003, <https://www.rfc-editor.org/info/rfc3526>.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC

4106, DOI 10.17487/RFC4106, June 2005, <https://www.rfc-editor.org/info/rfc4106>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC4308] Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308, DOI 10.17487/RFC4308, December 2005, <https://www.rfc-editor.org/info/rfc4308>.

[RFC4754] Fu, D. and J. Solinas, "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)", RFC 4754, DOI 10.17487/RFC4754, January 2007, <https://www.rfc-editor.org/info/rfc4754>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <https://www.rfc-editor.org/info/rfc4868>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <https://www.rfc-editor.org/info/rfc5116>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5903] Fu, D. and J. Solinas, "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2", RFC 5903, DOI 10.17487/RFC5903, June 2010, <https://www.rfc-editor.org/info/rfc5903>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/info/rfc8017>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017, <https://www.rfc-editor.org/info/rfc8221>.

[RFC8247] Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 8247, DOI 10.17487/RFC8247, September 2017, <https://www.rfc-editor.org/info/rfc8247>.

[RFC8603] Jenkins, M. and L. Zieglar, "Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile", RFC 8603, DOI 10.17487/RFC8603, May 2019, <https://www.rfc-editor.org/info/rfc8603>.

[RFC8784] Fluhrer, S., Kampanakis, P., McGrew, D., and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, DOI 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/info/rfc8784>.

[SP80056A] National Institute of Standards and Technology, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography", NIST Special Publication 800-56A, Revision 3, April 2018, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf>.

15.2. Informative References

[RFC8452] Gueron, S., Langley, A., and Y. Lindell, "AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption", RFC 8452, DOI 10.17487/RFC8452, April 2019, <https://www.rfc-editor.org/info/rfc8452>.

[SP80059] National Institute of Standards and Technology, "Guideline for Identifying an Information System as a National Security System", Special Publication 800-59 , August 2003, <https://csrc.nist.gov/publications/detail/sp/800-59/final>.

Authors' Addresses

Laura Corcoran
National Security Agency

Email: lscorco@nsa.gov

Michael Jenkins
National Security Agency

Email: mjjenki@cyber.nsa.gov