INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

暗号モジュール試験及び認証制度(JCMVP)

承認されたセキュリティ機能に関する仕様

(2020 年 1 月以降有効)

ASF-01

Approved Security Functions

令和元年 7 月 17 日

独立行政法人情報処理推進機構

目次

承認されたセキュリティ機能に関する仕様

令和元年 7 月 17 日

1. 目的

本規程は、独立行政法人情報処理推進機構 (以下「機構」という。) が、「暗号モジュール試験及び認証制度の基本規程」 (JCM-01) (以下「制度基本規程」という。) に基づいて、暗号モジュール認証機関 (以下「認証機関」という。) として実施する暗号モジュール試験及び認証制度 (JCMVP) (以下「本制度」という。) における承認されたセキュリティ機能に関する仕様等を定めるものである。

2. 承認されたセキュリティ機能

本章は、JCMVP 暗号モジュールセキュリティ要件に適用できる承認されたセキュリティ機能のリストを提供する。

公開鍵

＜署名＞

1. DSA
   FIPS PUB 186-4, Digital Signature Standard (DSS), July, 2013.
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
   注: 但し、署名生成に用いる p を 2048 ビット以上かつ q を 224 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。

2. ECDSA
   ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry :
   The Elliptic Curve Digital Signature Algorithm (ECDSA)
   注: 但し、署名生成に用いる楕円曲線の位数を 224 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。

3. ECDSA
   FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
   注: 但し、署名生成に用いる楕円曲線の位数を 224 ビット以上かつ使用するハッシュ関

数の出力長を 224 ビット以上とする。

4. ECDSA
   SEC 1: Elliptic Curve Cryptography (May 21, 2009 Version 2.0)
   http://www.secg.org/sec1-v2.pdf
   注 1: 但し、楕円曲線の位数を 160 ビット以上とする。
   注 2: 但し、署名生成に用いる楕円曲線の位数を 224 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。

5. RSASSA-PKCS1-v1_5
   PKCS#1 v2.2: RSA Cryptography Standard, October 27, 2012.
   https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf
   注 1: 但し、モジュラスとなる合成数を 1024 ビット以上とする。
   注 2: 但し、署名生成に用いるモジュラスとなる合成数を 2048 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。

6. RSASSA-PSS
   PKCS#1 v2.2: RSA Cryptography Standard, October 27, 2012.
   https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf
   注 1: 但し、モジュラスとなる合成数を 1024 ビット以上とする。
   注 2: 但し、署名生成に用いるモジュラスとなる合成数を 2048 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。

＜守秘＞

7. RSA-OAEP
   PKCS#1 v2.2: RSA Cryptography Standard, October 27, 2012.
   https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf
   注 1: 但し、モジュラスとなる合成数を 1024 ビット以上とする。
   注 2: 但し、暗号化についてはモジュラスとなる合成数を 2048 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。

共通鍵

＜128 ビットブロック暗号＞

1. AES
   FIPS PUB 197, Advanced Encryption Standard (AES), November 26, 2001
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

2. Camellia
   128 ビットブロック暗号 Camellia アルゴリズム仕様書 (第 2 版: 2001 年 9 月 26 日)
   https://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/06_01jspec.pdf

＜n-ビットブロック暗号の利用モード＞

3. Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR)
   SP 800-38A, Recommendation for Block Cipher Modes of Operation, December 2001.
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

＜128-ビットブロック暗号の利用モード＞

4. XTS
   SP 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, January 2010.
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf

＜ストリーム暗号＞

5. KCipher-2
   ストリーム暗号 KCipher-2 (仕様書 1.2 版)
   https://www.cryptrec.go.jp/cryptrec_13_spec_cypherlist_files/PDF/21_09spec_j_1.2.pdf

ハッシュ

1. Secure Hash Standard (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)
   FIPS PUB 180-4, Secure Hash Standard, August, 2015.
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

2. SHA-3 Hash Algorithms (SHA3-256, SHA3-384, SHA3-512)
   FIPS PUB 202, SHA-3 Standard, August, 2015.
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

3. SHA-3 Extendable-Output Functions (SHAKE128, SHAKE256)
   FIPS PUB 202, SHA-3 Standard, August, 2015.
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
   注: 但し、SHA-3 Extendable-Output Functions (SHAKE128 及び SHAKE256)の承認されたセキュリティ機能としての使用方法については、別途規定する。

メッセージ認証

1. HMAC (HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512/224, and HMAC-SHA-512/256)
   The Keyed-Hash Message Authentication Code, FIPS PUB 198-1, July 2008.
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf
   注: 但し、メッセージ認証子生成に用いる暗号鍵の鍵長は、112 ビット以上とする。

2. CMAC
   Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, May 2005 (Updated 10/6/2016).
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38B.pdf
   注: 但し、Triple DES を使用する CMAC は除く。

3. CCM
   Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, NIST Special Publication 800-38C, May 2004.
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

4. GCM/GMAC
   Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST Special Publication 800-38D, November 2007.
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

5. GCM-AES-XPN
   IEEE Standards Association, Standard for Local and metropolitan area networks, Media

Access Control (MAC) Security, Amendment 2: Extended Packet Numbering, 802.1AEbw-2013, February 12, 2013.

乱数生成器

1. Approved Random Number Generators
   3 章を参照

鍵確立手法

1. Approved Key Establishment Techniques
   4 章を参照

3. 承認された乱数生成器

本章は、JCMVP 暗号モジュールセキュリティ要件に適用できる承認された乱数生成器のリストを提供する。乱数生成器には、決定論的乱数生成器と、非決定論的乱数生成器の 2 種類がある。決定論的乱数生成器は、シードと呼ばれる初期値からビット列を生成するアルゴリズムから成り立つ。非決定論的乱数生成器は、人間による制御の範囲外であるいくつかの予測不可能な物理的発生源から成り立つ。

決定論的乱数生成器

1. Hash_DRBG, HMAC_DRBG and CTR_DRBG
   National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A Revision 1, June 2015.
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
   注: 但し、Triple DES を使用する CTR_DRBG は除く。

非決定論的乱数生成器

JCMVP 暗号モジュールセキュリティ要件に適用できる承認された非決定論的乱数生成器は無い。

4. 承認された鍵確立手法

本章は、JCMVP 暗号モジュールセキュリティ要件に適用できる承認された鍵確立手法のリストを提供する。

共通鍵確立手法

JCMVP 暗号モジュールセキュリティ要件に適用できる承認された共通鍵確立手法は無い。

公開鍵確立手法

＜鍵共有＞

1. DH

   National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Special Publication 800-56A Revision 3, April 2018.
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
   注 1: 但し、p を 2048 ビット以上かつ q を 224 ビット以上とする。
   注 2: 但し、ドメインパラメータは、FIPS 186-type に限る。

2. MQV

   National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Special Publication 800-56A Revision 3, April 2018.
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
   注 1: 但し、p を 2048 ビット以上かつ q を 224 ビット以上とする。
   注 2: 但し、ドメインパラメータは、FIPS 186-type に限る。

3. ECDH

   National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Special Publication 800-56A Revision 3, April 2018.
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
   注: 但し、楕円曲線の位数を 224 ビット以上とする。

4. ECDH

   SEC 1: Elliptic Curve Cryptography (May 21, 2009 Version 2.0)

   http://www.secg.org/sec1-v2.pdf

   注: 但し、楕円曲線の位数を 224 ビット以上とする。

5. ECMQV

   National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Special Publication 800-56A Revision 3, April 2018.

   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

   注: 但し、楕円曲線の位数を 224 ビット以上とする。

6. Key Establishment Schemes in NIST SP800-56B

   National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, Special Publication 800-56B Revision 2, March 2019.

   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf

   注: 但し、KMAC を使用する Key Confirmation は除く。

7. KDF

   National Institute of Standards and Technology, Recommendation for Key Derivation through Extraction-then-Expansion, Special Publication 800-56C Revision 1, April 2018.

   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf

   注: 但し、KMAC を使用する KDF は除く。

8. KDF

   National Institute of Standards and Technology, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), Special Publication 800-108, October 2009.

   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf

   注: 但し、Triple DES を使用する KDF は除く。

9. KDF

   National Institute of Standards and Technology, Recommendation for Password-Based Key Derivation, Special Publication 800-132, December 2010.

   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf

10. KDF

National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135 Revision 1, December 2011.

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf

注: 但し、TPM に基づく KDF は除く。

附　則（令和元年 7 月 17 日　2019 情セ技第 60 号・一部改正）

（適用期日）

本書は、令和 2 年 1 月 1 日から適用する。

改訂履歴

識別番号	ASF-01

改訂年月日	作成者・承認者	改訂内容
平成 19 年 5 月 15 日	上野・仲田	新規制定
平成 20 年 4 月 7 日	櫻井・占部	メッセージ認証に CCM を追加。決定論的乱数生成器に以下 3 種類を追加。 • ANSI X9.31 Appendix A.2.4 Using 3-Key Triple DES • ANSI X9.31 Appendix A.2.4 Using AES • Hash_DRBG, HMAC_DRBG and CTR_DRBG in NIST SP800-90
平成 21 年 2 月 24 日	櫻井・仲田	公開鍵確立手法 3. PSEC-KEM の仕様書の参照先を以下のとおり変更。 新：PSEC-KEM 仕様書 version 2.2 (平成 20 年 4 月 14 日) 旧：PSEC-KEM 仕様書 (2002 年 5 月 14 日) また、以下の乱数生成器を削除。 • Hash_DRBG, CTR_DRBG and OFB_DRBG in ISO/IEC 18031
平成 21 年 10 月 26 日	櫻井・仲田	• DSA の仕様の参照先から、ANSI X9.30 を削除。 • ECDSA の仕様の参照先に、ANS X9.62-2005 及び FIPS 186-3 を追加。 • DH の仕様の参照先である ANS X9.42 について、2001 年版から 2003 年版に参照先を更新。 • DH 及び ECDH の仕様の参照先に、NIST SP800-56A を追加。
平成 22 年 6 月 30 日	橋本・仲田	DSA の仕様の参照先である、FIPS PUB 186-2 with Change Notice 1 の URL を更新。

平成 24 年 2 月 29 日	橋本・仲田	共通鍵に XTS を追加、メッセージ認証に GCM/GMAC を追加。
平成 25 年 2 月 13 日	櫻井・仲田	• DSA の仕様の参照先に、FIPS 186-3 を追加。 • SHS の仕様の参照先を、FIPS 180-4 に変更。 • HMAC の仕様の参照先を、FIPS 198-1 に変更。 • Hash_DRBG, HMAC_DRBG, CTR_DRBG の仕様の参照先を、NIST SP800-90A に変更。 • ECDH(NIST SP800-56A)のスキームを限定する但し書きを削除。 • MQV、ECMQV を追加。 • Key Establishment Schemes in NIST SP800-56B を追加。 • 以下の仕様書に基づく KDF を追加 ➢ NIST SP800-56C ➢ NIST SP800-108 ➢ NIST SP800-132 ➢ NIST SP800-135 Rev.1
平成 25 年 6 月 21 日	櫻井・仲田	• 公開鍵 6., 7., 8.,及び 9. の仕様書の参照先を以下のとおり変更。 新：PKCS#1 v2.2: RSA Cryptography Standard, October 27, 2012. 旧：PKCS#1 v2.1: RSA Cryptography Standard, June 14, 2002. • 3-Key Triple DES の仕様書の参照先を NIST SP800-67 Revision 1 に変更。 • 暗号アルゴリズムの移行に伴う注記を記載。
平成 25 年 10 月 4 日	橋本・立石	• PKCS#1 v2.2 の参照先 URL を変更。
平成 26 年 4 月 1 日	橋本・立石	• DSA の仕様の参照先から、FIPS PUB 186-2 with Change Notice 1 を

		削除。 • DSA において、署名生成に用いる *p* を 2048 ビット以上かつ *q* を 224 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。 • ECDSA において、署名生成に用いる楕円曲線の位数を 224 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。 • ECDSA 及び ECDH の仕様の参照先である SEC1 について、Version 1.0 から Version 2.0 に参照先を変更。 • RSASSA-PKCS1-v1_5 及び RSASSA-PSS において、署名生成に用いるモジュラスとなる合成数を 2048 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。 • RSA-OAEP において、暗号化に用いるモジュラスとなる合成数を 2048 ビット以上かつ使用するハッシュ関数の出力長を 224 ビット以上とする。 • RSAES-PKCS1-v1_5 を承認されたセキュリティ機能から取り消す。 • 以下の 64 ビットブロック暗号を承認されたセキュリティ機能から取り消す ➢ CIPHERUNICORN-E ➢ Hierocrypt-L1 ➢ MISTY1 • 以下の 128 ビットブロック暗号を承認されたセキュリティ機能から取り消す ➢ CIPHERUNICORN-A

		➢ Hierocrypt-3 ➢ SC2000 • ストリーム暗号に KCipher-2 を追加。 • 以下のストリーム暗号を承認されたセキュリティ機能から取り消す ➢ MUGI ➢ MULTI-S01 ➢ 128-bit RC4 • RIPEMD-160 を承認されたセキュリティ機能から取り消す。 • HMAC において、メッセージ認証子生成に用いる暗号鍵の鍵長を 112 ビット以上とする。 • DH の仕様の参照先から、ANS X9.42-2003 を削除。 • DH 及び MQV において、*p* を 2048 ビット以上かつ *q* を 224 ビット以上とする。 • ECDH 及び ECMQV において、楕円曲線の位数を 224 ビット以上とする。 • PSEC-KEM を承認されたセキュリティ機能から取り消す。 • SP800-56B において、モジュラスとなる合成数を 2048 ビット以上とする。
平成 30 年 6 月 22 日	櫻井・江口	• DSA、ECDSA の仕様の参照先を、FIPS 186-4 に変更。 • KCipher-2 の仕様の参照先を、仕様書 1.2 版に変更。 • SHA-3、SHA-3 Extendable Output Functions を追加。 • Hash_DRBG, HMAC_DRBG, CTR_DRBG の仕様の参照先を、NIST SP800-90A Revision 1 に変

		更。 • DH, MQV, ECDH, ECMQV の仕様の参照先を、NIST SP800-56A Revision 3 に変更。 • Key Establishment Schemes in NIST SP800-56B の仕様の参照先を、NIST SP800-56B Revision 1 に変更。 • 承認された鍵確立手法 7.の仕様書の参照先を以下のとおり変更。 新：NIST SP 800-56C Revision 1, April, 2018. 旧：NIST SP 800-56C, November, 2011. • NIST 発行の FIPS 及び SP800 文書の URL を更新
令和元年 7 月 11 日	櫻井・江口	• GCM-AES-XPN を追加。 • 承認された鍵確立手法 6.の仕様書の参照先を以下のとおり変更。 新:NIST SP 800-56B Revision 2, March, 2019. 旧：NIST SP 800-56B Revision 1, September, 2014.
令和元年 7 月 17 日	櫻井・江口	• 3-key Triple DES を削除。 • CMAC, CTR_DRBG, NIST SP 800-108 に基づく KDF に、3-key Triple DES の削除に伴う注記を記載。