CAVP Mapping

Version 1.0

17 November 2016

This document serves as a guideline for CCTLs to determine if a CAVP certificate is acceptable as evidence of meeting some PP/cPP assurance activities. This document shows which cryptographic algorithm validation list, as well as the modes, states, key sizes, etc. (depending on the requirements and selections), are required to meet the applicable Security Functional Requirement (SFR).

Key:

v - inclusive 'or' used to form expressions
^ - 'and' used to form expressions
or - 'or' used to join expressions

SFR	CAVP Validation List and Description/Notes
FCS_CKM - Key Generation	
RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	RSA Validation List FIPS 186-4: 186-4KEY(gen): PGM(ProvRandom) ^ ((2048 SHA(256 v 384 v 512)) v (3072 SHA(256 v 384 v 512))) or PGM(ProbRandom) ^ (2048 v 3072) ^ PPTT(C.2 v C.3) or PGM(ProvPrimeCondition) ^ (2048 SHA(256 v 384 v 512)) v (3072 SHA(256 v 384 v 512)) or PGM(BothPrimeCondition) ^ ((2048 SHA(256 v 384 v 512)) v (3072 SHA(256 v 384 v 512))) ^ PPTT(C.2 v C.3) or PGM(ProbPrimeCondition) ^ (2048) v (3072) ^ PPTT(C.2 v C.3)
ECC schemes using "NIST curves that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	ECDSA Validation List FIPS 186-4 PKG: Curves ((P-256 v P-384 v P-521) and PKV: Curves ((P-256 v P-384 v P521) **NOTE**: Hash algorithms following each of the relevant curves must include what has been selected in FCS_COP

FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1	DSA Validation List FIPS 186-4: KeyPairGen: [(2048,256) v (3072,256)]
FCS_CKM - Key Generation WLAN Symmetric	
Generate symmetric cryptographic keys in accordance with PRF-384 meeting the following: [IEEE 802.11-2012]	HMAC Validation List HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS v KS=BS v KS>BS) and Other Validations: WiFi CERTIFIEDTM **NOTE**: The WiFi CertifiedTM testing only addresses a portion of the Assurance Activity testing.
Generate symmetric cryptographic keys in accordance with PRF-704 meeting the following: [IEEE 802.11ac-2013]	HMAC Validation List HMAC-SHA384 (Key Sizes Ranges Tested: KS<BS v KS=BS v KS>BS) and Other Validations: WiFi CERTIFIEDTM **NOTE**: The WiFi CertifiedTM testing only addresses a portion of the Assurance Activity testing.
FCS_CKM - Key Distribution WLAN	
Decrypt Group Temporal Key (GTK) in accordance with a specified cryptographic key distribution method [AES Key Wrap in an EAPOL-Key frame] that meets the following: [NIST SP 800-38F, IEEE 802.11-2012 for the packet format and timing considerations] and does not expose the cryptographic keys	AES Validation List KW (AD ^ (AES-128 v AES-256) ^ ((CMAC (Verification) ^ (KS: 128)) v HMAC Validation List HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS v KS=BS v KS>BS)) And Other Validations: WiFi CERTIFIEDTM
FCS_CKM - Key Establishment	
[RSA-based key establishment schemes] that meet the following: [NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment	No CAVP exists, must be described in TSS – See FIPS 140-2 I.G. D.4: Vendor Affirmation - http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

Schemes Using Integer Factorization Cryptography”]	SHS Validation List - Hash algorithms as applicable DRBG Validation List - Supported Random Bit Generators (DRBG) RSA Validation List - An RSA key pair generation algorithm in FIPS 186-4
[Elliptic curve-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”]	If using 800-56A KDF, KAS Validation List ECC: SCHEMES [(FullUnified v FullMQV v EphemeralUnified v OnePassUnified v OnePassMQV v OnePassDH v StaticUnified)] ^ For each SCHEME listed: (EC: P-256 ^ (SHA256 v SHA384 v SHA512)) ^ (ED: P-384 ^ (SHA384 v SHA512)) ^ (EE: P-521 ^ SHA512)] or If using a non 800-56A KDF, Component Validation List (CVL) Component Validated: All of SP800-56A EXCEPT KDF "ECC" and a KARole of either Initiator or Responder (depending on the PP and TOE's role) and listing NIST Curves P-256, P-384, P-521 equal to what is claimed in the SFRs **NOTE**: In the future an applicable CVL for SP800-135 KDFs will also be required to meet included protocol SFRs. or If using a non 800-56A KDF, KAS Validation List ECC: SCHEMES [(FullUnified v FullMQV v EphemeralUnified v OnePassUnified v OnePassMQV v OnePassDH v StaticUnified)] ^ For each SCHEME listed: (EC: P-256 ^ (SHA256 v SHA384 v SHA512)) ^ (ED: P-384 ^ (SHA384 v SHA512)) ^ (EE: P-512 ^ SHA512)] **NOTE**: In the future an applicable CVL for SP800-135 KDFs will also be required to meet included protocol SFRs. **NOTE:** The component validation called “Section 5.7.1.2: ECC CDH Primitive” does **NOT** suffice for the validation “All of SP800-56A EXCEPT KDF”. The testing for the component

	validation "Section 5.7.1.2: ECC CDH Primitive" does not include many of the tests that are in the component validation "All of SP800-56A EXCEPT KDF" and in the assurance activity.
[Finite field-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"]	If using a 800-56A KDF, KAS Validation List FFC: SCHEMES [(HYBRID1 v MQV2 v EPHEM v HYBRID1FLOW v MQV1 v ONEFLOW v STATIC) ^ ((FB: SHA256 v SHA384 v SHA512) v (FC: SHA256 v SHA384 v SHA512))] or If using a non 800-56A KDF, Component Validation List (CVL) Component Validated: All of SP800-56A EXCEPT KDF "FFC" and a KARole of either Initiator or Responder (depending on the PP and TOE's role). **NOTE**: In the future an applicable CVL for SP800-135 KDFs will also be required to meet included protocol SFRs. or If using a non 800-56A KDF, KAS Validation List FFC: SCHEMES [(HYBRID1 v MQV2 v EPHEM HYBRID1FLOW v MQV1 v ONEFLOW v STATIC) ^ ((FB: SHA256 v SHA384 v SHA512) v (FC: SHA256 v SHA384 v SHA512))] **NOTE**: In the future an applicable CVL for SP800-135 KDFs will also be required to meet included protocol SFRs.
FCS_CKM – Key Support REK NIST SP 800-108 key derivation	KBKDF (SP800-108) Validation List MACSupported([HMACSHA1] v [HMACSHA224] [HMACSHA256] v [HMACSHA384] v [HMACSHA512])
FCS_COP - Cryptographic Operation – AES Encryption/Decryption	
AES-CBC (as defined in NIST SP 800-38A)	AES Validation List CBC (e/d; 128 v 192 v 256)
AES-GCM (as defined in NIST SP 800-38D)	AES Validation List GCM (KS: AES_128(e/d)) v (KS: AES_192(e/d)) v GCM (KS: AES_256(e/d)) **NOTE**: If GCM listing specifies: "IV Generated: (Internally)", the GCM implementation must use the same DRBG that is referenced in FCS_RBG_EXT.1

AES-XTS (as defined in NIST SP 800-38E)	AES Validation List XTS((KS: XTS_128(e/d) ^ KS: XTS_256(e/d))
AES-CCM (as defined in NIST SP 800-38C)	AES Validation List CCM(KS: 128 ^ 192 ^ 256)
AES Key Wrap (KW) (as defined in NIST SP 800-38F)	AES Validation List KW ((AE v AD) ^(AES-128 v AES-256)
AES Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F)	AES Validation List KWP KWP ((AE v AD) ^(AES-128 v AES-256)
AES-CCMP (as defined in NIST SP 800-38C and IEEE 802.11-2012)	AES Validation List CCM(KS: 128 ^ 256)) and Other Validations (For WLAN and Mobile only): WiFi CERTIFIEDTM
AES-CCMP-256 (as defined in NIST SP800-38C and IEEE 802.11ac-2013)	AES Validation List CCM(KS: 256) ^ and Other Validations (For WLAN and Mobile only): WiFi CERTIFIEDTM
AES-GCMP-256 (as defined in NIST SP800-38D and IEEE 802.11ac-2013)	AES Validation List GCM(KS: 256) ^ And Other Validations (For WLAN and Mobile only): WiFi CERTIFIEDTM
FCS_COP – Cryptographic Operation - Signature Algorithms	
RSA schemes using cryptographic key sizes [of 2048-bit or greater] that meet the following: [FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 4 Note: Both Generation and Verification are required	RSA Validation List FIPS 186-4: ALG [ANSIX9.31] v [RSASSA-PSS] v [RSASSA-PKCS1_V1_5] For each ALG listed: SIG(gen) (2048 SHA (256 v 384 v 512)) v (3072 SHA(256 v 384 v 512)) ^ SIG(ver) (2048 SHA (256 v 384 v 512)) v (3072 SHA (256 v 384 v 512))
ECDSA schemes using [“NIST curves” P-256, P-384	ECDSA Validation List

and [selection: P-521, no other curves]] that meet the following: [FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5] Note: Both Generation and Verification are required	FIPS186-4: PKG: CURVES(P-256 ^ P-384 ^ P-521) ^ SigGen: CURVES(P-256: (SHA (256 v 384 v 512)) ^ P-384: (SHA (256 v 384 v 512)) ^ P-521: (SHA (256 v 384 v 512)) ^ PKV: CURVES(P-256 ^ P-384 ^ P-521) v PKV: CURVES(ALL-P) ^ SigVer: CURVES(P-256: (256 v 384 v 512)) ^ P-384: (SHA (256 v 384 v 512)) ^ P-521: (256 v 384 v 512))
FCS_COP – Cryptographic Operation - Hashing Algorithms	
SHS that meets: FIPS Pub 180-4 or ISO/IEC 10118-3:2004. SHA Bit-oriented Mode Byte-oriented Mode	SHS Validation List SHA-1 (BIT) v SHA-1 (BYTE-only) ^ SHA-256 (BIT) v SHA-256 (BYTE-only) v SHA-384 (BIT) v SHA-384 (BYTE-only) v SHA-512 (BIT) v SHA-512 (BYTE-only)
FCS_COP – Cryptographic Operation - Keyed Hash	
HMAC that meets : FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-4, “Secure Hash Standard or ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2” Application Note: The selection in this requirement must be consistent with the key size specified for the size of the keys used in conjunction with the keyed-hash message authentication.	HMAC Validation List HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS v KS=BS v KS>BS) ^ HMAC-SHA256(Key Sizes Ranges Tested: KS<BS v KS=BS v KS>BS) v HMAC-SHA384(Key Sizes Ranges Tested: KS<BS v KS=BS v KS>BS) v HMAC-SHA512(Key Sizes Ranges Tested: KS<BS v KS=BS v KS>BS) Note: Each HMAC should have a corresponding hash function
FCS_RBG – Random Bit Generation	
Hash_DRBG(any)	DRBG Validation List Hash_Based DRBG: [(SHA-1 v SHA-256 v SHA-384 v SHA-512) (SHA Val#)] **NOTE**: DRBG Val# must correspond to SHA-1 v SHA-256 v SHA-384 v SHA-512 Val#(s)
HMAC_DRBG(any)	DRBG Validation List HMAC_Based DRBG: [(SHA-1 v SHA-256 v SHA-384 v SHA-512) (HMAC Val#)] **NOTE**: DRBG Val# must correspond to HMAC-SHA1 v HMAC-SHA256 v HMAC-SHA384 v HMAC-SHA512 Val#(s)
CTR_DRBG(AES)	DRBG Validation List CTR_DRBG[(AES-128 v AES-192 v AES-256) **NOTE**: DRBG Val# must correspond to AES-128 v AES-192 v AES-256 Val#(s)]