CAVP Mapping
Version 2.0
25 June 2018

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).

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: Key Generation: Provable Random Primes: Mod 2048 SHA or Mod 3072: SHA-1 or SHA-256 or SHA-384 or SHA-512 or Key Generation: Public Key Exponent: Fixed (10001) Probable Random Primes: Mod lengths: 2048 or 3072 (bits) Primality Tests: C.2 or C.3 or Key Generation: Public Key Exponent: Random Probable Primes with Conditions: Mod lengths: 2048 or 3072 (bits) Primality Tests: C.2 or C.3 or Key Generation: Public Key Exponent: Fixed (10001) Provable Primes with Conditions: Mod 2048 SHA or Mod 3072: SHA-1 or SHA-256 or SHA-384 or SHA-512 or Provable and Probable Primes with Conditions: Mod 2048 SHA or Mod 3072: SHA-1 or SHA-256 or

	SHA-384 or SHA-512 Primality Tests: C.2 or 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 Key Pair Generation: Curves: P-256 or P-384 or P-521 AND Public Key Validation: Curves: P-256 or P-384 or P-521
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: KeyPair: L = 2048, N = 256 or L = 3072, N = 256 **NOTE**: Must have matching SHS and DRBG certificates
FFC Scheme using Diffie-Hellman Group 14 or FFC using safe prime groups	No NIST CAVP, CCTL must perform all assurance/evaluation activities.
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 < Block Size or Key Sizes > Block Size or Key Sizes = Block Size 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 < Block Size or Key Sizes > Block Size or Key Sizes = Block Size and

	Other Validations: WiFi CERTIFIEDTM **NOTE**: The WiFi CertifiedTM testing only addresses a portion of the Assurance Activity testing.
FCS_CKM - Key Distribution WLAN	
The TSF shall distribute Group Temporal Key (GTK) in accordance with a specified cryptographic key distribution method: [selection: AES Key Wrap in an EAPOL-Key frame, AES Key Wrap with Padding 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.	**For WLAN Client EP:** AES Validation List AES-KW: Modes: Decrypt, Encrypt CIPHK transformation direction: Forward Key Lengths: 128 or 256 (bits) or AES-KWP: Modes: Decrypt, Encrypt Key Lengths: 128 or 256 (bits) AND AES-CMAC Verification: AES-128 AND HMAC Validation List HMAC-SHA1 Key Sizes < Block Size or Key Sizes > Block Size or Key Sizes = Block Size AND Other Validations: WiFi CERTIFIEDTM **FOR WLAN AS PP**: This SFR to be met by obtaining the appropriate NIST CAVP certifications and performing the tests detailed in the AA or by obtaining the NIST CAVP certification along with the Wi-Fi Alliance WPA2 Certification.
FCS_CKM - Key Establishment	
[RSA-based key establishment schemes] that meet the following: [NIST Special Publication 800-56B,	No CAVP exists, must be described in TSS – See FIPS 140-2 I.G. D.4: Vendor Affirmation -

"Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"]	http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf 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"]	KAS Validation List or Component Validation List (CVL) KAS ECC: SCHEMES [(FullUnified or FullMQV or EphemeralUnified or OnePassUnified or OnePassMQV or OnePassDH or StaticUnified)] and Key Agreement Roles: Initiator or Responder Parameter Sets: EC: Curve: P-256 SHA: SHA-256 or SHA-384 or SHA-512 ED: Curve: P-384 SHA: SHA-384 or SHA-512 EE: Curve: P-521 SHA: SHA-512 **NOTE**: If using an 800-56A KDF, the KAS Validation List is used. If using a non 800-56A KDF, the Component Validation List (CVL) is used. **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 "ECC CDH: Primitive" does **NOT** suffice for the validation "All of SP800-56A EXCEPT KDF" as 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	KAS Validation List or Component Validation List (CVL) KAS FFC: SCHEMES [(dhHybrid1 or MQV2 or dhEphem or dhHybrid1Flow or MQV1 or DhOneFlow or dhStatic)

Establishment Schemes Using Discrete Logarithm Cryptography"]	Key Agreement Roles: Initiator or Responder Parameter Sets: FB: SHA: SHA-256 or SHA-384 or SHA-512 FC: SHA: SHA-256 or SHA-384 or SHA-512 **NOTE**: If using an 800-56A KDF, the KAS Validation List is used. If using a non 800-56A KDF, the Component Validation List (CVL) is used. **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	KDF Validation List Counter or Double Pipeline Iteration or Feedback: MACs: CMAC-AES-128 or CMAC-AES-256 or HMAC-SHA-256 or HMAC-SHA-384 or HMAC-SHA-512 Counter Location: After Fixed Data or Before Fixed Data or In the Middle of Fixed Data
FCS_COP - Cryptographic Operation – AES Encryption/Decryption	
AES-CBC (as defined in NIST SP 800-38A)	AES Validation List AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 128 or 192 or 256 (bits)
AES-GCM (as defined in NIST SP 800-38D)	AES Validation List AES-GCM: Modes: Decrypt, Encrypt IV Generation: External or Internal Key Lengths: 128 or 192 or 256 (bits) **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 AES-XTS: Key Size: 128: Modes: Decrypt, Encrypt Key Size: 256: Modes: Decrypt, Encrypt
AES-CTR	AES Validation List AES-CTR: Counter Source: Internal or External Key Lengths: 128 or 256 (bits)

AES-CCM (as defined in NIST SP 800-38C)	AES Validation List AES-CCM: Key Lengths: 128 or 256 (bits)
AES Key Wrap (KW) (as defined in NIST SP 800-38F)	AES Validation List AES-KW: Modes: Decrypt, Encrypt Key Lengths: 128 or 256 (bits)
AES Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F)	AES Validation List AES-KWP: Modes: Decrypt, Encrypt Key Lengths: 128 or 256 (bits)
AES-CCMP (as defined in NIST SP 800-38C and IEEE 802.11-2012)	AES Validation List AES-CCM: Key Lengths: 128 or 256 (bits) and Other Validations (for WLAN only) WiFi CERTIFIEDTM
AES-CCMP-256 (as defined in NIST SP800-38C and IEEE 802.11ac-2013)	AES Validation List AES-CCM: Key Lengths: 256 (bits) AND Other Validations (for WLAN only) WiFi CERTIFIEDTM
AES-GCMP-256 (as defined in NIST SP800-38D and IEEE 802.11ac-2013)	AES Validation List AES-GCM: Modes: Decrypt, Encrypt IV Generation: External or Internal Key Lengths: 256 (bits) AND Other Validations (for WLAN 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: Signature Generation PSS: Mod 2048: SHA-1 or SHA-256 or SHA-384 or

	SHA-512 or Mod 3072: SHA-1 or SHA-256 or SHA-384 or SHA-512 And Signature Verification PSS: Mod 2048: SHA-1: Salt Length: 160 (bits) or SHA-256: Salt Length: 256 (bits) or SHA-384: Salt Length: 384 (bits) or SHA-512: Salt Length: 512 (bits) Or Mod 3072: SHA-1: Salt Length: 160 (bits) or SHA-256: Salt Length: 256 (bits) or SHA-384: Salt Length: 384 (bits) or SHA-512: Salt Length: 512 (bits) OR Signature Generation PKCS1.5: Mod 2048 SHA: SHA-1 or SHA-256 or SHA-384 or SHA-512 Mod 3072 SHA: SHA-1 or SHA-256 or SHA-384 or SHA-512 And Signature Verification PKCS1.5: Mod 2048 SHA: SHA-1 or SHA-256 or SHA-384 or SHA-512 Mod 3072 SHA: SHA-1 or SHA-256 or SHA-384 or SHA-512
ECDSA schemes using [“NIST curves” P-256, P-384 and P-521] that meet the following: [FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5] Note: Both Generation and Verification are required	ECDSA Validation List FIPS186-4: Signature Generation: P-256 SHA: SHA-256 or SHA-384 or SHA-512 P-384 SHA: SHA-256 or SHA-384 or SHA-512 P-521 SHA: SHA-256 or SHA-384 or SHA-512 Signature Verification: P-256 SHA: SHA-256 or SHA-384 or SHA-512 P-384 SHA: SHA-256 or SHA-384 or SHA-512

	P-521 SHA: SHA-256 or SHA-384 or SHA-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: or SHA-256: or SHA-384: or SHA-512:
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-SHA-1: Key Sizes < Block Size Key Sizes > Block Size Key Sizes = Block Size HMAC-SHA2-256: Key Sizes < Block Size Key Sizes > Block Size Key Sizes = Block Size HMAC-SHA2-384: Key Sizes < Block Size Key Sizes > Block Size Key Sizes = Block Size HMAC-SHA2-512: Key Sizes < Block Size Key Sizes > Block Size Key Sizes = Block Size Note: Each HMAC must have a corresponding Hash (SHS) function
FCS_RBG – Random Bit Generation	
Hash_DRBG(any)	DRBG Validation List Hash based: Modes: SHA-1 or SHA-256 or SHA-384 or SHA-512 **NOTE**: DRBG Val# must correspond to SHA-1 or SHA-256 or SHA-384 or SHA-512 Val#(s)
HMAC_DRBG(any)	DRBG Validation List HMAC based: Modes: SHA-1 or SHA-256 or SHA-384 or SHA-512 **NOTE**: DRBG Val# must correspond to SHA-1 or SHA-256 or SHA-384 or SHA-512 Val#(s)
CTR_DRBG(AES)	DRBG Validation List

	Counter: Modes: AES-128 or AES-256 **NOTE**: DRBG Val# must correspond to AES-128 or AES-256 Val#(s)]