securosys

Primus HSM Supported Algorithms and Functions

Published April 2024
Release V3.0

Address

Max-Högger-Strasse 2
8048 Zurich
Switzerland

Phone & Fax

Phone: + 41 44 552 31 00
Fax: + 41 44 552 31 99

Email

Email 1: info@securosys.com
Website: www.securosys.com

+ Primus HSM Supported Algorithms and Functions

Algorithm	Description
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption; Modes: ECB, CBC, CTR Functions: Key Wrap, Key Unwrap; Modes: ECB, CBC Key sizes: 128, 192, 256 bits
AES-CMAC	[SP 800-38B] Functions: MAC Generation, MAC Verification Key sizes: 128, 192, 256 bits
AES-GCM	[FIPS 197, SP 800-38D] Functions: Authenticated Encryption, Authenticated Decryption, GMAC Generation, GMAC Verification Key sizes: 128, 192, 256 bits IV-Construction: RBG-based Construction with 96-bit random field and 0-bit free field. A unique IV is constructed for each usage. For line encryption an IV is calculated for each direction (send/receive) and increased after each packet. Note: The IV is generated internally at its entirety randomly as per technique 2 of IG A.5.
AES-KW	[SP 800-38F] Functions: Key Wrap, Key Unwrap Modes: KW, KWP Key sizes: 128, 192, 256
DRBG	[SP 800-90A] HMAC DRBG with internal function SHA-512 CTR DRBG with internal function AES-256
DSA	[FIPS 186-4] Functions: PQG Generation, Key Pair Generation, Signature Generation, Signature Verification Key sizes: 2048, 3072 bits
ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification, Public Key Validation Curves/Key sizes: P-224, P-256, P-384, P-521 (Strength: 112, 128, 192, 260)
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512
KAS (FFC, ECC)	[SP 800-56Ar1] Parameter sets/Key sizes: FC, EB, EC, ED, EE Modes: dhStatic responder, Static Unified responder Scheme: SHA2 Note: Key establishment methodology provides between 112 and 256 bits of encryption strength
KDF	[SP 800-108] Modes: Counter, Feedback, Double Pipeline Iteration Mode PRFs: CMAC(AES-128/192/256), HMAC (SHA-1, 224, 256, 384, 512)

Algorithm	Description
KTS (Symmetric)	[SP800-38F] Functions: Key Wrap, Key Unwrap Variants: 38D: AES-GCM (256 bits) 38F: AES-KW, AES-KWP Key Transport – Provides between 128 and 256 bits of encryption strength.
RSA	[FIPS 186-4, ANSI X9.31-1998, and PKCS #1 v2.1 (PSS and PKCS1.5)] Functions: Key Pair Generation, Signature Generation, Signature Verification, Key Wrap, Key Unwrap, Encrypt, Decrypt Key sizes: 512, 1024 (non-FIPS mode only) Key sizes: 2048, 3072, 4096, 7680, 8192 bits Some RSA-4096 functions are listed here but not displayed on RSA Cert. #2946. These are vendor-affirmed, as CAVP does not provide testing for these functions.
SHA	[FIPS 180-4, FIPS 202] Functions: Digital Signature Generation, Digital Signature Verification, component of HMAC and HMAC_DRBG, general hashing SHA sizes: SHA-1 verification only, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512
Triple-DES (TDES)	[SP 800-67] Functions: Decryption; Modes: TECB, TCBC Functions: Encryption, Key Wrap, Key Unwrap; Modes: CBC, ECB Key sizes: 3-key
Double-DES (DDES)	[SP 800-20] Functions: Encryption, Decryption, Key Wrap, Key Unwrap Modes: CBC, ECB Key sizes: 2-key
ECDSA SigGen Component	[FIPS 186-4] Curves/Key sizes: P-224, P-256, P-384, P-521
KAS Component	[SP 800-56A Section 5.7.1.2 ECC CDH Primitive] Parameter sets/Key sizes: EB, EC, ED, EE
RSA DP	[SP 800-56B] Key sizes: 2048 bits
RSA SP	[FIPS 186-4, ANSI X9.31-1998, and PKCS #1 v2.1 (PSS and PKCS1.5)] Key sizes: 2048 bits
CKG	[SP800-133] Asymmetric Key Generation (SP800-133 §6) Symmetric Key Generation (SP800-133 §7: Direct output from DRBG)
KTS (RSA)	[SP 800-56B] Functions: Key Wrap, Key Unwrap Key sizes: 2048, 3072, 4096 bits Key {Agreement | Transport} – Provides 112 to 150 bits of encryption strength. Wrap Methods: RSASVE, RSA-OAEP

Algorithm	Description
KDFs, Password-based	[SP 800-132] PRFs: HMAC (SHA-1, SHA2 224/256/384/512, SHA3 224/256/384/512)
NDRNG	[FIPS IG G.13] The NDRNG sole purpose is an entropy source for the DRBG built according to SP800-90A.
ECC operations with non-NIST curves.	[FIPS IG A.2] Elliptic Curve operations with non-NIST curves, as follows: Curve: — Security Strength: Brainpool 224r1, 256r1, 320r1, 384r1, 512r1 — 112, 128, 160, 192, 256 Frp 256v1 — 128 X9.62p239v1, v2, v3 — 119 secp224k1, 256k1 — 112, 128
MD5	RFC1321 Function: 128-bit hash
Camelia	https://info.isl.ntt.co.jp/crypt/eng/camellia/dl/01espec.pdf Function: Encryption / Decryption Key sizes: 128,192,256 bits
SHA-1	[FIPS 180-4, FIPS 202] Function: Hash, for other operations than verification
DH	PKCS3 Function: Key agreement, superseded by KAS (FFC)
CBC-MAC	FIPS PUB 113 Function: Message authentication (superseded by AES-CMAC)
Securosys TRNG	Securosys hardware specification Function: Non-deterministic random number generation (NDRNG)
Securosys RNG	Securosys hardware specification Function: Performant deterministic random number generation (AES-128)
ISS	Iota.org Function: IOTA Signature Scheme
EdDSA	RFC8032 Function: EC digital signature algorithm using Edwards curve (ED25519)
EdDH	RFC8031 Function: EC Diffie Hellman using Edwards curve (X25519)
SLIP-0010	https://github.com/satoshilabs/slips/blob/master/slip-0010.md Function: Seed import, Key derivation Curves: SECP256k1, NIST P-256
ChaCha	https://cr.yp.to/chacha/chacha-20080128.pdf Function: Stream cipher

Algorithm	Description
Keccak 1600	[FIPS 202] Function: Hash
Kerl	Iota.org Function: Hash
RIPEMD160	ISO/IEC 10118-3:2018 Function: Hash
Poly1305	https://cr.yp.to/mac/poly1305-20050329.pdf Function: Message Authentication Code
ChaCha 20 – Poly1305	RFC 7905 Function: Authenticated encryption / decryption
BLS12-381	RFC draft-irtf-cfrg-bls-signature-04 - draft-irtf-cfrg-bls-signature-02 (ietf.org) Function: Sign & Verify according with ETH 2.0
Cardano ED key derivation	https://docs.cardano.org/projects/cardano-wallet/en/latest/About-Address-Derivation.html Function: Authenticated encryption / decryption
SHAKE	[FIPS 202] Function: Extendable output Modes: SHAKE-128, SHAKE-256
CRYSTALS-Kyber	[FIPS 203] Function: Key Pair Generation, Key encapsulation Modes: FIPS Round 3 Submission
CRYSTALS-Dilith-ium	[FIPS 204] Function: Key Pair Generation, Signature Generation, Signature Verification Modes: FIPS Round-3 Submission
SPHINCS+	[FIPS 205] Function: Key Pair Generation, Signature Generation, Signature Verification Modes: FIPS Round-3 Submission