OpenSSL Available Algorithms

Digests: Legacy: RSA-MD4 => MD4 RSA-MD5 => MD5 RSA-MDC2 => MDC2 RSA-RIPEMD160 => RIPEMD160 RSA-SHA1 => SHA1 RSA-SHA1-2 => RSA-SHA1 RSA-SHA224 => SHA224 RSA-SHA256 => SHA256 RSA-SHA3-224 => SHA3-224 RSA-SHA3-256 => SHA3-256 RSA-SHA3-384 => SHA3-384 RSA-SHA3-512 => SHA3-512 RSA-SHA384 => SHA384 RSA-SHA512 => SHA512 RSA-SHA512/224 => SHA512-224 RSA-SHA512/256 => SHA512-256 RSA-SM3 => SM3 BLAKE2b512 BLAKE2s256 id-rsassa-pkcs1-v1_5-with-sha3-224 => SHA3-224 id-rsassa-pkcs1-v1_5-with-sha3-256 => SHA3-256 id-rsassa-pkcs1-v1_5-with-sha3-384 => SHA3-384 id-rsassa-pkcs1-v1_5-with-sha3-512 => SHA3-512 MD4 md4WithRSAEncryption => MD4 MD5 MD5-SHA1 md5WithRSAEncryption => MD5 MDC2 mdc2WithRSA => MDC2 ripemd => RIPEMD160 RIPEMD160 ripemd160WithRSA => RIPEMD160 rmd160 => RIPEMD160 SHA1 sha1WithRSAEncryption => SHA1 SHA224 sha224WithRSAEncryption => SHA224 SHA256 sha256WithRSAEncryption => SHA256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 SHA384 sha384WithRSAEncryption => SHA384 SHA512 SHA512-224 sha512-224WithRSAEncryption => SHA512-224 SHA512-256 sha512-256WithRSAEncryption => SHA512-256 sha512WithRSAEncryption => SHA512 SHAKE128 SHAKE256 SM3 sm3WithRSAEncryption => SM3 ssl3-md5 => MD5 ssl3-sha1 => SHA1 whirlpool Provided: { 1.3.6.1.4.1.1722.12.2.2.8, BLAKE2S-256, BLAKE2s256 } @ default { 2.16.840.1.101.3.4.2.10, SHA3-512 } @ default { 2.16.840.1.101.3.4.2.6, SHA-512/256, SHA2-512/256, SHA512-256 } @ default { 2.16.840.1.101.3.4.2.4, SHA-224, SHA2-224, SHA224 } @ default { 1.3.14.3.2.26, SHA-1, SHA1, SSL3-SHA1 } @ default { 2.16.840.1.101.3.4.2.7, SHA3-224 } @ default { 2.16.840.1.101.3.4.2.9, SHA3-384 } @ default { 1.3.36.3.2.1, RIPEMD, RIPEMD-160, RIPEMD160, RMD160 } @ default { 2.16.840.1.101.3.4.2.3, SHA-512, SHA2-512, SHA512 } @ default { 2.16.840.1.101.3.4.2.5, SHA-512/224, SHA2-512/224, SHA512-224 } @ default { 2.16.840.1.101.3.4.2.12, SHAKE-256, SHAKE256 } @ default { 2.16.840.1.101.3.4.2.2, SHA-384, SHA2-384, SHA384 } @ default { 1.2.156.10197.1.401, SM3 } @ default { 2.16.840.1.101.3.4.2.8, SHA3-256 } @ default { 1.2.840.113549.2.5, MD5, SSL3-MD5 } @ default { 2.16.840.1.101.3.4.2.1, SHA-256, SHA2-256, SHA256 } @ default { 1.3.6.1.4.1.1722.12.2.1.16, BLAKE2B-512, BLAKE2b512 } @ default MD5-SHA1 @ default { 2.16.840.1.101.3.4.2.11, SHAKE-128, SHAKE128 } @ default { SHA-256/192, SHA2-256/192, SHA256-192 } @ default KECCAK-224 @ default KECCAK-256 @ default KECCAK-384 @ default KECCAK-512 @ default { KECCAK-KMAC-128, KECCAK-KMAC128 } @ default { KECCAK-KMAC-256, KECCAK-KMAC256 } @ default NULL @ default

Symmetric Ciphers: Legacy: RC5 => RC5-CBC AES-128-CBC AES-128-CBC-HMAC-SHA1 AES-128-CBC-HMAC-SHA256 id-aes128-CCM AES-128-CFB AES-128-CFB1 AES-128-CFB8 AES-128-CTR AES-128-ECB id-aes128-GCM AES-128-OCB AES-128-OFB AES-128-XTS AES-192-CBC id-aes192-CCM AES-192-CFB AES-192-CFB1 AES-192-CFB8 AES-192-CTR AES-192-ECB id-aes192-GCM AES-192-OCB AES-192-OFB AES-256-CBC AES-256-CBC-HMAC-SHA1 AES-256-CBC-HMAC-SHA256 id-aes256-CCM AES-256-CFB AES-256-CFB1 AES-256-CFB8 AES-256-CTR AES-256-ECB id-aes256-GCM AES-256-OCB AES-256-OFB AES-256-XTS aes128 => AES-128-CBC aes128-wrap => id-aes128-wrap aes128-wrap-pad => id-aes128-wrap-pad aes192 => AES-192-CBC aes192-wrap => id-aes192-wrap aes192-wrap-pad => id-aes192-wrap-pad aes256 => AES-256-CBC aes256-wrap => id-aes256-wrap aes256-wrap-pad => id-aes256-wrap-pad ARIA-128-CBC ARIA-128-CCM ARIA-128-CFB ARIA-128-CFB1 ARIA-128-CFB8 ARIA-128-CTR ARIA-128-ECB ARIA-128-GCM ARIA-128-OFB ARIA-192-CBC ARIA-192-CCM ARIA-192-CFB ARIA-192-CFB1 ARIA-192-CFB8 ARIA-192-CTR ARIA-192-ECB ARIA-192-GCM ARIA-192-OFB ARIA-256-CBC ARIA-256-CCM ARIA-256-CFB ARIA-256-CFB1 ARIA-256-CFB8 ARIA-256-CTR ARIA-256-ECB ARIA-256-GCM ARIA-256-OFB aria128 => ARIA-128-CBC aria192 => ARIA-192-CBC aria256 => ARIA-256-CBC bf => BF-CBC BF-CBC BF-CFB BF-ECB BF-OFB blowfish => BF-CBC CAMELLIA-128-CBC CAMELLIA-128-CFB CAMELLIA-128-CFB1 CAMELLIA-128-CFB8 CAMELLIA-128-CTR CAMELLIA-128-ECB CAMELLIA-128-OFB CAMELLIA-192-CBC CAMELLIA-192-CFB CAMELLIA-192-CFB1 CAMELLIA-192-CFB8 CAMELLIA-192-CTR CAMELLIA-192-ECB CAMELLIA-192-OFB CAMELLIA-256-CBC CAMELLIA-256-CFB CAMELLIA-256-CFB1 CAMELLIA-256-CFB8 CAMELLIA-256-CTR CAMELLIA-256-ECB CAMELLIA-256-OFB camellia128 => CAMELLIA-128-CBC camellia192 => CAMELLIA-192-CBC camellia256 => CAMELLIA-256-CBC cast => CAST5-CBC cast-cbc => CAST5-CBC CAST5-CBC CAST5-CFB CAST5-ECB CAST5-OFB ChaCha20 ChaCha20-Poly1305 des => DES-CBC DES-CBC DES-CFB DES-CFB1 DES-CFB8 DES-ECB DES-EDE DES-EDE-CBC DES-EDE-CFB des-ede-ecb => DES-EDE DES-EDE-OFB DES-EDE3 DES-EDE3-CBC DES-EDE3-CFB DES-EDE3-CFB1 DES-EDE3-CFB8 des-ede3-ecb => DES-EDE3 DES-EDE3-OFB DES-OFB des3 => DES-EDE3-CBC des3-wrap => id-smime-alg-CMS3DESwrap desx => DESX-CBC DESX-CBC id-aes128-CCM id-aes128-GCM id-aes128-wrap id-aes128-wrap-pad id-aes192-CCM id-aes192-GCM id-aes192-wrap id-aes192-wrap-pad id-aes256-CCM id-aes256-GCM id-aes256-wrap id-aes256-wrap-pad id-smime-alg-CMS3DESwrap idea => IDEA-CBC IDEA-CBC IDEA-CFB IDEA-ECB IDEA-OFB rc2 => RC2-CBC rc2-128 => RC2-CBC rc2-40 => RC2-40-CBC RC2-40-CBC rc2-64 => RC2-64-CBC RC2-64-CBC RC2-CBC RC2-CFB RC2-ECB RC2-OFB RC4 RC4-40 RC4-HMAC-MD5 RC5-CBC RC5-CFB RC5-ECB RC5-OFB seed => SEED-CBC SEED-CBC SEED-CFB SEED-ECB SEED-OFB sm4 => SM4-CBC SM4-CBC SM4-CFB SM4-CTR SM4-ECB SM4-OFB Provided: { 1.2.392.200011.61.1.1.1.4, CAMELLIA-256-CBC, CAMELLIA256 } @ default { 1.2.156.10197.1.104.2, SM4, SM4-CBC } @ default { 1.2.410.200046.1.1.12, ARIA-256-CBC, ARIA256 } @ default { 2.16.840.1.101.3.4.1.22, AES-192-CBC, AES192 } @ default { 2.16.840.1.101.3.4.1.4, AES-128-CFB } @ default {

1.2.410.200046.1.1.38, ARIA-192-CCM } @ default { 1.2.410.200046.1.1.1, ARIA-128-ECB } @ default { 2.16.840.1.101.3.4.1.2, AES-128-CBC, AES128 } @ default { 2.16.840.1.101.3.4.1.24, AES-192-CFB } @ default { 1.2.392.200011.61.1.1.1.2, CAMELLIA-128-CBC, CAMELLIA128 } @ default { 1.2.410.200046.1.1.35, ARIA-192-GCM } @ default { 2.16.840.1.101.3.4.1.42, AES-256-CBC, AES256 } @ default { 2.16.840.1.101.3.4.1.28, AES-192-WRAP-PAD, AES192-WRAP-PAD, id-aes192-wrap-pad } @ default { 1.2.410.200046.1.1.36, ARIA-256-GCM } @ default { 1.3.111.2.1619.0.1.2, AES-256-XTS } @ default { 2.16.840.1.101.3.4.1.8, AES-128-WRAP-PAD, AES128-WRAP-PAD, id-aes128-wrap-pad } @ default { 1.2.840.113549.1.9.16.3.6, DES3-WRAP, id-smime-alg-CMS3DESwrap } @ default { 2.16.840.1.101.3.4.1.48, AES-256-WRAP-PAD, AES256-WRAP-PAD, id-aes256-wrap-pad } @ default { 1.2.156.10197.1.104.3, SM4-OFB, SM4-OFB128 } @ default { 2.16.840.1.101.3.4.1.25, AES-192-WRAP, AES192-WRAP, id-aes192-wrap } @ default { 2.16.840.1.101.3.4.1.41, AES-256-ECB } @ default { 0.3.4401.5.3.1.9.49, CAMELLIA-256-CTR } @ default { 1.2.410.200046.1.1.2, ARIA-128-CBC, ARIA128 } @ default { 2.16.840.1.101.3.4.1.6, aes-128-gcm, id-aes128-GCM } @ default { 0.3.4401.5.3.1.9.41, CAMELLIA-256-ECB } @ default { 2.16.840.1.101.3.4.1.44, AES-256-CFB } @ default { 1.2.156.10197.1.104.4, SM4-CFB, SM4-CFB128 } @ default { 0.3.4401.5.3.1.9.4, CAMELLIA-128-CFB } @ default { 1.2.410.200046.1.1.39, ARIA-256-CCM } @ default { 1.2.410.200046.1.1.14, ARIA-256-OFB } @ default { 2.16.840.1.101.3.4.1.46, aes-256-gcm, id-aes256-GCM } @ default { 0.3.4401.5.3.1.9.9, CAMELLIA-128-CTR } @ default { 2.16.840.1.101.3.4.1.23, AES-192-OFB } @ default { 1.2.156.10197.1.104.1, SM4-ECB } @ default { 2.16.840.1.101.3.4.1.7, aes-128-ccm, id-aes128-CCM } @ default { 2.16.840.1.101.3.4.1.47, aes-256-ccm, id-aes256-CCM } @ default { 1.2.410.200046.1.1.7, ARIA-192-CBC, ARIA192 } @ default { 2.16.840.1.101.3.4.1.45, AES-256-WRAP, AES256-WRAP, id-aes256-wrap } @ default { 1.2.410.200046.1.1.15, ARIA-256-CTR } @ default { 1.2.410.200046.1.1.3, ARIA-128-CFB } @ default { 1.2.410.200046.1.1.34, ARIA-128-GCM } @ default { 1.2.410.200046.1.1.6, ARIA-192-ECB } @ default { 2.16.840.1.101.3.4.1.26, aes-192-gcm, id-aes192-GCM } @ default { 0.3.4401.5.3.1.9.29, CAMELLIA-192-CTR } @ default { 0.3.4401.5.3.1.9.43, CAMELLIA-256-OFB } @ default { 1.2.410.200046.1.1.37, ARIA-128-CCM } @ default { 2.16.840.1.101.3.4.1.27, aes-192-ccm, id-aes192-CCM } @ default { 1.3.14.3.2.17, DES-EDE, DES-EDE-ECB } @ default { 1.2.410.200046.1.1.11, ARIA-256-ECB } @ default { 1.3.111.2.1619.0.1.1, AES-128-XTS } @ default { 2.16.840.1.101.3.4.1.5, AES-128-WRAP, AES128-WRAP, id-aes128-wrap } @ default { 2.16.840.1.101.3.4.1.3, AES-128-OFB } @ default { 0.3.4401.5.3.1.9.3, CAMELLIA-128-OFB } @ default { 0.3.4401.5.3.1.9.1, CAMELLIA-128-ECB } @ default { 1.2.840.113549.3.7, DES-EDE3-CBC, DES3 } @ default { 0.3.4401.5.3.1.9.44, CAMELLIA-256-CFB } @ default { 1.2.410.200046.1.1.10, ARIA-192-CTR } @ default { 0.3.4401.5.3.1.9.23, CAMELLIA-192-OFB } @ default { 0.3.4401.5.3.1.9.24, CAMELLIA-192-CFB } @ default { 1.2.410.200046.1.1.9, ARIA-192-OFB } @ default { 1.2.410.200046.1.1.13, ARIA-256-CFB } @ default { 2.16.840.1.101.3.4.1.1, AES-128-ECB } @ default { 1.2.410.200046.1.1.8, ARIA-192-CFB } @ default { 1.2.156.10197.1.104.7, SM4-CTR } @ default { 2.16.840.1.101.3.4.1.43, AES-256-OFB } @ default { 1.2.410.200046.1.1.4, ARIA-128-OFB } @ default { 1.2.392.200011.61.1.1.1.3, CAMELLIA-192-CBC, CAMELLIA192 } @ default { 0.3.4401.5.3.1.9.21, CAMELLIA-192-ECB } @ default { 1.2.410.200046.1.1.5, ARIA-128-CTR } @ default { 2.16.840.1.101.3.4.1.21, AES-192-ECB } @ default NULL @ default AES-128-CBC-CTS @ default AES-192-CBC-CTS @ default AES-256-CBC-CTS @ default AES-256-CFB1 @ default AES-192-CFB1 @ default AES-128-CFB1 @ default AES-256-CFB8 @ default AES-192-CFB8 @ default AES-128-CFB8 @ default AES-256-CTR @ default AES-192-CTR @ default AES-128-CTR @ default AES-256-OCB @ default AES-192-OCB @ default AES-128-OCB @ default AES-128-SIV @ default AES-192-SIV @ default AES-256-SIV @ default AES-128-GCM-SIV @ default AES-192-GCM-SIV @ default AES-256-GCM-SIV @ default { AES-256-WRAP-INV, AES256-WRAP-INV } @ default { AES-192-WRAP-INV, AES192-WRAP-INV } @ default { AES-128-WRAP-INV, AES128-WRAP-INV } @ default { AES-256-WRAP-PAD-INV, AES256-WRAP-PAD-INV } @ default { AES-192-WRAP-PAD-INV, AES192-WRAP-PAD-INV } @ default { AES-128-WRAP-PAD-INV, AES128-WRAP-PAD-INV } @ default AES-128-CBC-HMAC-SHA1 @ default AES-256-CBC-HMAC-SHA1 @ default AES-128-CBC-HMAC-SHA256 @ default AES-256-CBC-HMAC-SHA256 @ default ARIA-256-CFB1 @ default ARIA-192-CFB1 @ default ARIA-128-CFB1 @ default ARIA-256-CFB8 @ default ARIA-192-CFB8 @ default ARIA-128-CFB8 @ default CAMELLIA-128-CBC-CTS @ default CAMELLIA-192-CBC-CTS @ default CAMELLIA-256-CBC-CTS @ default CAMELLIA-256-CFB1 @ default CAMELLIA-192-CFB1 @ default CAMELLIA-128-CFB1 @ default CAMELLIA-256-CFB8 @ default CAMELLIA-192-CFB8 @ default CAMELLIA-128-CFB8 @ default { DES-EDE3, DES-EDE3-ECB } @ default DES-EDE3-OFB @ default DES-EDE3-CFB @ default DES-EDE3-CFB8 @ default DES-EDE3-CFB1 @ default DES-EDE-CBC @ default DES-EDE-OFB @ default DES-EDE-CFB @ default { 1.2.156.10197.1.104.8, SM4-GCM } @ default { 1.2.156.10197.1.104.9, SM4-CCM } @ default { 1.2.156.10197.1.104.10, SM4-XTS } @ default ChaCha20 @ default ChaCha20-Poly1305 @ default

Provided KDFs and PDFs: HKDF @ default TLS13-KDF @ default SSKDF @ default { 1.2.840.113549.1.5.12, PBKDF2 } @ default PKCS12KDF @ default SSHKDF @ default { X942KDF-CONCAT, X963KDF } @ default TLS1-PRF @ default KBKDF @ default { X942KDF, X942KDF-ASN1 } @ default { 1.3.6.1.4.1.11591.4.11, id-scrypt, SCRYPT } @ default KRB5KDF @ default HMAC-DRBG-KDF @ default ARGON2I @ default ARGON2D @ default ARGON2ID @ default

Provided MACs: { 1.3.6.1.4.1.1722.12.2.1, BLAKE2BMAC } @ default { 1.3.6.1.4.1.1722.12.2.2, BLAKE2SMAC } @ default CMAC @ default { 1.0.9797.3.4, GMAC } @ default HMAC @ default { 2.16.840.1.101.3.4.2.19, KMAC-128, KMAC128 } @ default { 2.16.840.1.101.3.4.2.20, KMAC-256, KMAC256 } @ default SIPHASH @ default POLY1305 @ default

Provided Asymmetric Encryption: { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default { 1.2.156.10197.1.301, SM2 } @ default

Provided Key Exchange: { 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default { 1.3.101.110, X25519 } @ default { 1.3.101.111, X448 } @ default HKDF @ default TLS1-PRF @ default { 1.3.6.1.4.1.11591.4.11, id-scrypt, SCRYPT } @ default ECDH @ default

Provided Signatures: { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default { 1.2.840.10040.4.3, 1.3.14.3.2.27, DSA-SHA, DSA-SHA-1, DSA-SHA1, DSA-SHA1-old, dsaWithSHA, dsaWithSHA1, dsaWithSHA1-old } @ default { 1.3.101.112, ED25519 } @ default { 1.3.101.113, ED448 } @ default { 1.2.156.10197.1.301, SM2 } @ default CMAC @ default HMAC @ default SIPHASH @ default POLY1305 @ default { 2.16.840.1.101.3.4.3.1, DSA-SHA2-224, DSA-SHA224, dsa_with_SHA224 } @ default { 2.16.840.1.101.3.4.3.2, DSA-SHA2-256, DSA-SHA256, dsa_with_SHA256 } @ default { 1.2.840.1.101.3.4.3.3, DSA-SHA2-384, DSA-SHA384, dsa_with_SHA384, id-dsa-with-sha384 } @ default { 1.2.840.1.101.3.4.3.4, DSA-SHA2-512, DSA-SHA512, dsa_with_SHA512, id-dsa-with-sha512 } @ default { 2.16.840.1.101.3.4.3.5, DSA-SHA3-224, dsa_with_SHA3-224, id-dsa-with-sha3-224 } @ default { 2.16.840.1.101.3.4.3.6, DSA-SHA3-256, dsa_with_SHA3-256, id-dsa-with-sha3-256 } @ default { 2.16.840.1.101.3.4.3.7, DSA-SHA3-384, dsa_with_SHA3-384, id-dsa-with-sha3-384 } @ default { 2.16.840.1.101.3.4.3.8, DSA-SHA3-512, dsa_with_SHA3-512, id-dsa-with-sha3-512 } @ default { 1.3.36.3.3.1.2, ripemd160WithRSA, RSA-RIPEMD160 } @ default { 1.2.840.113549.1.1.5, RSA-SHA-1, RSA-SHA1, sha1WithRSAEncryption } @ default { 1.2.840.113549.1.1.14, RSA-SHA2-224, RSA-SHA224, sha224WithRSAEncryption } @ default { 1.2.840.113549.1.1.11, RSA-SHA2-256, RSA-SHA256, sha256WithRSAEncryption } @ default { 1.2.840.113549.1.1.12, RSA-SHA2-384, RSA-SHA384, sha384WithRSAEncryption } @ default { 1.2.840.113549.1.1.13, RSA-SHA2-512, RSA-SHA512, sha512WithRSAEncryption } @ default { 1.2.840.113549.1.1.15, RSA-SHA2-512/224, RSA-SHA512-224, sha512-224WithRSAEncryption } @ default { 1.2.840.113549.1.1.16, RSA-SHA2-512/256, RSA-SHA512-256, sha512-256WithRSAEncryption } @ default { 2.16.840.1.101.3.4.3.13, id-rsassa-pkcs1-v1_5-with-sha3-224, RSA-SHA3-224 } @ default { 2.16.840.1.101.3.4.3.14, id-rsassa-pkcs1-v1_5-with-sha3-256, RSA-SHA3-256 } @ default { 2.16.840.1.101.3.4.3.15, id-rsassa-pkcs1-v1_5-with-sha3-384, RSA-SHA3-384 } @ default { 2.16.840.1.101.3.4.3.16, id-rsassa-pkcs1-v1_5-with-sha3-512, RSA-SHA3-512 } @ default { 1.2.156.10197.1.504, RSA-SM3, sm3WithRSAEncryption } @ default ED25519ph @ default ED25519ctx @ default ED448ph @ default ECDSA @ default { 1.2.840.10045.4.1, ECDSA-SHA-1, ECDSA-SHA1, ecdsa-with-SHA1 } @ default { 1.2.840.10045.4.3.1, ECDSA-SHA2-224, ECDSA-SHA224, ecdsa-with-SHA224 } @ default { 1.2.840.10045.4.3.2, ECDSA-SHA2-256, ECDSA-SHA256, ecdsa-with-SHA256 } @ default { 1.2.840.10045.4.3.3, ECDSA-SHA2-384, ECDSA-SHA384, ecdsa-with-SHA384 } @ default { 1.2.840.10045.4.3.4, ECDSA-SHA2-512, ECDSA-SHA512, ecdsa-with-SHA512 } @ default { 2.16.840.1.101.3.4.3.9, ECDSA-SHA3-224, ecdsa_with_SHA3-224, id-ecdsa-with-sha3-224 } @ default { 2.16.840.1.101.3.4.3.10, ECDSA-SHA3-256, ecdsa_with_SHA3-256, id-ecdsa-with-sha3-256 } @ default { 2.16.840.1.101.3.4.3.11, ECDSA-SHA3-384, ecdsa_with_SHA3-384, id-ecdsa-with-sha3-384 } @ default { 2.16.840.1.101.3.4.3.12, ECDSA-SHA3-512, ecdsa_with_SHA3-512, id-ecdsa-with-sha3-512 } @ default

Provided Key encapsulation: { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default { 1.3.101.110, X25519 } @ default { 1.3.101.111, X448 } @ default

Provided Key managers: Name: OpenSSL RSA implementation Type: Provider Algorithm IDs: { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default Name: OpenSSL PKCS#3 DH implementation Type: Provider Algorithm IDs: { 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default Name: OpenSSL DSA implementation Type: Provider Algorithm IDs: { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default Name: OpenSSL EC implementation Type: Provider Algorithm IDs: { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default Name: OpenSSL RSA-PSS implementation Type: Provider Algorithm IDs: { 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default Name: OpenSSL X9.42 DH implementation Type: Provider Algorithm IDs: { 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default Name: OpenSSL X25519 implementation Type: Provider Algorithm IDs: { 1.3.101.110, X25519 } @ default Name: OpenSSL X448 implementation Type: Provider Algorithm IDs: { 1.3.101.111, X448 } @ default Name: OpenSSL ED25519 implementation Type: Provider Algorithm IDs: { 1.3.101.112, ED25519 } @ default Name: OpenSSL ED448 implementation Type: Provider Algorithm IDs: { 1.3.101.113, ED448 } @ default Name: OpenSSL SM2 implementation Type: Provider Algorithm IDs: { 1.2.156.10197.1.301, SM2 } @ default Name: OpenSSL HKDF via EVP_PKEY implementation Type: Provider Algorithm IDs: HKDF @ default Name: OpenSSL TLS1_PRF via EVP_PKEY implementation Type: Provider Algorithm IDs: TLS1-PRF @ default Name: OpenSSL SCRYPT via EVP_PKEY implementation Type: Provider Algorithm IDs: { 1.3.6.1.4.1.11591.4.11, id-scrypt, SCRYPT } @ default Name: OpenSSL CMAC via EVP_PKEY implementation Type: Provider Algorithm IDs: CMAC @ default Name: OpenSSL HMAC via EVP_PKEY implementation Type: Provider Algorithm IDs: HMAC @ default Name: OpenSSL SIPHASH via EVP_PKEY implementation Type: Provider Algorithm IDs: SIPHASH @ default Name: OpenSSL POLY1305 via EVP_PKEY implementation Type: Provider Algorithm IDs: POLY1305 @ default

Provided ENCODERs: { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=text) { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=der,structure=type-specific) { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ de-

fault (provider=default,fips=yes,output=pem,structure=type-specific) {
1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=msblob)
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=pvk)
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=der,structu
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=pem,struct
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=der,structu
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=pem,struct
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=der,structu
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=pem,struct
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=der,structu
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=pem,struct
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=der,structu
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,output=pem,struct
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=text)
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=der,structure=typ
specific) { 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=pem,stru
specific) { 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=der,struc
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=pem,structure=En
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=der,structure=Pri
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=pem,structure=Pr
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=der,structure=Sub
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=pem,structure=Su
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=der,structure=dh)
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=pem,structure=dh
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=der,structure=pkc
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,output=pem,structure=pk
{ 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=text) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=der,structure=type-specific) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=pem,structure=type-specific) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=msblob) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=pvk) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=der,structure=EncryptedPrivateKeyInfo) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=pem,structure=EncryptedPrivateKeyInfo) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=der,structure=PrivateKeyInfo) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=pem,structure=PrivateKeyInfo) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,output=der,structure=SubjectPublicKeyInfo)

{ 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-
old } @ default (provider=default,fips=yes,output=pem,structure=SubjectPublicKeyInfo)
{ 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-
old } @ default (provider=default,fips=yes,output=der,structure=dsa) {
1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-
old } @ default (provider=default,fips=yes,output=pem,structure=dsa) {
1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=text)
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=der,structure=type-
specific) { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=pem,structure=
specific) { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=blob)
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=der,structure=Encrypte
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=pem,structure=Encrypt
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=der,structure=PrivateK
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=pem,structure=Private
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=der,structure=SubjectP
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=pem,structure=Subject
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=der,structure=ec)
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=pem,structure=ec)
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=der,structure=X9.62)
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,output=pem,structure=X9.62)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default
(provider=default,fips=yes,output=text) { 1.2.840.113549.1.1.10, RSA-PSS,
RSASSA-PSS, rsassaPss } @ default (provider=default,fips=yes,output=der,structure=EncryptedPrivateKeyIn
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default
(provider=default,fips=yes,output=pem,structure=EncryptedPrivateKeyInfo)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default
(provider=default,fips=yes,output=der,structure=PrivateKeyInfo)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default
(provider=default,fips=yes,output=pem,structure=PrivateKeyInfo)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default
(provider=default,fips=yes,output=der,structure=SubjectPublicKeyInfo)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default
(provider=default,fips=yes,output=pem,structure=SubjectPublicKeyInfo)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default
(provider=default,fips=yes,output=der,structure=pkcs1) { 1.2.840.113549.1.1.10,
RSA-PSS, RSASSA-PSS, rsassaPss } @ default (provider=default,fips=yes,output=pem,structure=pkcs1)
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=text)
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=der,struct
specific) { 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default
(provider=default,fips=yes,output=pem,structure=type-specific) {
1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=der,structu
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=pem,struc
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=der,struct
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=pem,struc
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=der,struct
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=pem,struc

```
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=der,struct
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=pem,struc
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=der,struct
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,output=pem,struc
{ 1.3.101.110, X25519 } @ default (provider=default,fips=yes,output=text) {
1.3.101.110, X25519 } @ default (provider=default,fips=yes,output=der,structure=EncryptedPrivateKeyInfo)
{ 1.3.101.110, X25519 } @ default (provider=default,fips=yes,output=pem,structure=EncryptedPrivateKeyInfo
{ 1.3.101.110, X25519 } @ default (provider=default,fips=yes,output=der,structure=PrivateKeyInfo)
{ 1.3.101.110, X25519 } @ default (provider=default,fips=yes,output=pem,structure=PrivateKeyInfo)
{ 1.3.101.110, X25519 } @ default (provider=default,fips=yes,output=der,structure=SubjectPublicKeyInfo)
{ 1.3.101.110, X25519 } @ default (provider=default,fips=yes,output=pem,structure=SubjectPublicKeyInfo)
{ 1.3.101.111, X448 } @ default (provider=default,fips=yes,output=text) {
1.3.101.111, X448 } @ default (provider=default,fips=yes,output=der,structure=EncryptedPrivateKeyInfo)
{ 1.3.101.111, X448 } @ default (provider=default,fips=yes,output=pem,structure=EncryptedPrivateKeyInfo)
{ 1.3.101.111, X448 } @ default (provider=default,fips=yes,output=der,structure=PrivateKeyInfo)
{ 1.3.101.111, X448 } @ default (provider=default,fips=yes,output=pem,structure=PrivateKeyInfo)
{ 1.3.101.111, X448 } @ default (provider=default,fips=yes,output=der,structure=SubjectPublicKeyInfo)
{ 1.3.101.111, X448 } @ default (provider=default,fips=yes,output=pem,structure=SubjectPublicKeyInfo)
{ 1.3.101.112, ED25519 } @ default (provider=default,fips=yes,output=text) {
1.3.101.112, ED25519 } @ default (provider=default,fips=yes,output=der,structure=EncryptedPrivateKeyInfo)
{ 1.3.101.112, ED25519 } @ default (provider=default,fips=yes,output=pem,structure=EncryptedPrivateKeyIn
{ 1.3.101.112, ED25519 } @ default (provider=default,fips=yes,output=der,structure=PrivateKeyInfo)
{ 1.3.101.112, ED25519 } @ default (provider=default,fips=yes,output=pem,structure=PrivateKeyInfo)
{ 1.3.101.112, ED25519 } @ default (provider=default,fips=yes,output=der,structure=SubjectPublicKeyInfo)
{ 1.3.101.112, ED25519 } @ default (provider=default,fips=yes,output=pem,structure=SubjectPublicKeyInfo)
{ 1.3.101.113, ED448 } @ default (provider=default,fips=yes,output=text) {
1.3.101.113, ED448 } @ default (provider=default,fips=yes,output=der,structure=EncryptedPrivateKeyInfo)
{ 1.3.101.113, ED448 } @ default (provider=default,fips=yes,output=pem,structure=EncryptedPrivateKeyInfo)
{ 1.3.101.113, ED448 } @ default (provider=default,fips=yes,output=der,structure=PrivateKeyInfo)
{ 1.3.101.113, ED448 } @ default (provider=default,fips=yes,output=pem,structure=PrivateKeyInfo)
{ 1.3.101.113, ED448 } @ default (provider=default,fips=yes,output=der,structure=SubjectPublicKeyInfo)
{ 1.3.101.113, ED448 } @ default (provider=default,fips=yes,output=pem,structure=SubjectPublicKeyInfo)
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=text)
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=der,structure=type-
specific) { 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=pem,structure=type-
specific) { 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=blob)
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=der,structure=EncryptedPrivateKey
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=pem,structure=EncryptedPrivateKey
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=der,structure=PrivateKeyInfo)
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=pem,structure=PrivateKeyInfo)
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=der,structure=SubjectPublicKeyInfo
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,output=pem,structure=SubjectPublicKeyInf
```

```
Provided DECODERs: { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption }
@ default (provider=default,fips=yes,input=der,structure=PrivateKeyInfo) {
1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,input=der,structure
```

{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,input=der,structur
specific) { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default
(provider=default,fips=yes,input=der,structure=rsa) { 1.2.840.113549.1.1.1,
2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,input=msblob)
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default (provider=default,fips=yes,input=pvk)
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,input=der,structure=Priva
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,input=der,structure=Subj
{ 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,input=der,structure=type-
specific) { 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ default (provider=default,fips=yes,input=der,structu
{ 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,input=der,structure=PrivateKeyInfo)
{ 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,input=der,structure=SubjectPublicKeyInfo)
{ 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,input=der,structure=type-specific) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,input=der,structure=dsa) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,input=msblob) { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ default (provider=default,fips=yes,input=pvk) { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,input=der,structure=PrivateKeyInfo) {
1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,input=der,structure=SubjectPub
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,input=der,structure=type-
specific) { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default (provider=default,fips=yes,input=der,structure=e
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default (provider=default,fips=yes,input=der,structure=PrivateKeyInfo) { 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ default (provider=default,fips=yes,input=der,structure=SubjectPublicKeyInfo) {
1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,input=der,structur
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,input=der,structu
{ 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,input=der,structu
specific) { 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ default (provider=default,fips=yes,input=der,structure=dhx) { 1.3.101.110, X25519 } @ default (provider=default,fips=yes,input=der,structure=PrivateKeyInfo) {
1.3.101.110, X25519 } @ default (provider=default,fips=yes,input=der,structure=SubjectPublicKeyInfo)
{ 1.3.101.111, X448 } @ default (provider=default,fips=yes,input=der,structure=PrivateKeyInfo)
{ 1.3.101.111, X448 } @ default (provider=default,fips=yes,input=der,structure=SubjectPublicKeyInfo)
{ 1.3.101.112, ED25519 } @ default (provider=default,fips=yes,input=der,structure=PrivateKeyInfo)
{ 1.3.101.112, ED25519 } @ default (provider=default,fips=yes,input=der,structure=SubjectPublicKeyInfo)
{ 1.3.101.113, ED448 } @ default (provider=default,fips=yes,input=der,structure=PrivateKeyInfo)
{ 1.3.101.113, ED448 } @ default (provider=default,fips=yes,input=der,structure=SubjectPublicKeyInfo)
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,input=der,structure=PrivateKeyInfo)
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,input=der,structure=SubjectPublicKeyInfo)
{ 1.2.156.10197.1.301, SM2 } @ default (provider=default,fips=no,input=der,structure=type-
specific) DER @ default (provider=default,fips=yes,input=der,structure=SubjectPublicKeyInfo)

DER @ default (provider=default,fips=yes,input=pem) DER @ default (provider=default,fips=yes,input=der,structure=EncryptedPrivateKeyInfo)

Provided STORE LOADERs: file @ default