OpenSSL Available Algorithms

Digests: Legacy: gost-mac md_gost12_256 md_gost12_512 md_gost94 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 gost-mac gost-mac-12 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 kuznyechik-ctr-acpkm-omac kuznyechik-mac magma-mac MD4 md4WithRSAEncryption => MD4 MD5 MD5-SHA1 md5WithRSAEncryption => MD5 md_gost12_256 md_gost12_512 md_gost94 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 streebog256 => md_gost12_256 streebog512 => md_gost12_512 whirlpool Provided: { 2.16.840.1.101.3.4.2.8, SHA3-256 } @ default { 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 { 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 { 2.16.840.1.101.3.4.2.8, SHA3-256 } @ fips { 2.16.840.1.101.3.4.2.10, SHA3-512 } @ fips { 2.16.840.1.101.3.4.2.6, SHA-512/256, SHA2-512/256, SHA512-

256 } @ fips { 2.16.840.1.101.3.4.2.4, SHA-224, SHA2-224, SHA224 } @ fips { 1.3.14.3.2.26, SHA-1, SHA1, SSL3-SHA1 } @ fips { 2.16.840.1.101.3.4.2.7, SHA3-224 } @ fips { 2.16.840.1.101.3.4.2.9, SHA3-384 } @ fips { 2.16.840.1.101.3.4.2.3, SHA-512, SHA2-512, SHA512 } @ fips { 2.16.840.1.101.3.4.2.5, SHA-512/224, SHA2-512/224, SHA512-224 } @ fips { 2.16.840.1.101.3.4.2.12, SHAKE-256, SHAKE256 } @ fips { 2.16.840.1.101.3.4.2.2, SHA-384, SHA2-384, SHA384 } @ fips { 2.16.840.1.101.3.4.2.1, SHA-256, SHA2-256, SHA256 } @ fips { 2.16.840.1.101.3.4.2.11, SHAKE-128, SHAKE128 } @ fips { KECCAK-KMAC-128, KECCAK-KMAC128 } @ fips { KECCAK-KMAC-256, KECCAK-KMAC256 } @ fips { 1.3.36.3.2.1, RIPEMD, RIPEMD-160, RIPEMD160, RMD160 } @ legacy { 1.0.10118.3.0.55, whirlpool } @ legacy { 2.5.8.3.101, MDC2 } @ legacy { 1.2.840.113549.2.4, MD4 } @ legacy

Symmetric Ciphers: Legacy: gost89 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 gost89 gost89-cbc gost89-cnt gost89-cnt-12 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 kuznyechik-cbc kuznyechik-cfb kuznyechik-ctr kuznyechik-ctr-acpkm kuznyechik-ctr-acpkm-omac kuznyechik-ecb kuznyechik-kexp15 kuznyechik-mgm kuznyechik-ofb magma-cbc magma-ctr magma-ctr-acpkm magma-ctr-acpkm-omac magma-ecb magma-kexp15 magma-mgm 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 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: { 0.3.4401.5.3.1.9.21, CAMELLIA-192-ECB } @ default { 1.2.410.200046.1.1.5, ARIA-128-CTR } @ default { 1.2.840.113549.3.7, DES-EDE3-CBC, DES3 } @ default { 1.2.410.200046.1.1.7, ARIA-192-CBC, ARIA192 } @ default { 1.2.410.200046.1.1.3, ARIA-128-CFB } @ default { 0.3.4401.5.3.1.9.29, CAMELLIA-192-CTR } @ default { 2.16.840.1.101.3.4.1.6, aes-128-gcm, id-aes128-GCM } @ default { 2.16.840.1.101.3.4.1.26, aes-192-gcm, id-aes192-GCM } @ default { 0.3.4401.5.3.1.9.43, CAMELLIA-256-OFB } @ default { 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 { 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 { 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 { 1.2.410.200046.1.1.34, ARIA-128-GCM } @ default { 1.2.410.200046.1.1.6, ARIA-192-ECB } @ 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 { 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 { 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 { 1.2.840.113549.3.7, DES-EDE3-CBC, DES3 } @ fips { 2.16.840.1.101.3.4.1.6, aes-128-gcm, id-aes128-GCM } @ fips { 2.16.840.1.101.3.4.1.26, aes-192-gcm, id-aes192-GCM } @ fips { 2.16.840.1.101.3.4.1.22, AES-192-CBC, AES192 } @ fips { 2.16.840.1.101.3.4.1.4, AES-128-CFB } @ fips { 2.16.840.1.101.3.4.1.2, AES-128-CBC, AES128 } @ fips { 2.16.840.1.101.3.4.1.24, AES-192-CFB } @ fips { 2.16.840.1.101.3.4.1.42, AES-256-CBC, AES256 } @ fips { 2.16.840.1.101.3.4.1.28, AES-192-WRAP-PAD, AES192-WRAP-PAD, id-aes192-wrap-pad } @ fips { 1.3.111.2.1619.0.1.2, AES-256-XTS } @ fips { 2.16.840.1.101.3.4.1.8, AES-128-WRAP-PAD, AES128-WRAP-PAD, id-aes128-wrap-pad } @ fips { 2.16.840.1.101.3.4.1.48, AES-256-WRAP-PAD, AES256-WRAP-PAD, id-aes256-wrap-pad } @ fips { 2.16.840.1.101.3.4.1.25, AES-192-WRAP, AES192-WRAP, id-aes192-wrap } @ fips { 2.16.840.1.101.3.4.1.41, AES-256-ECB } @ fips { 2.16.840.1.101.3.4.1.44, AES-256-CFB } @ fips { 2.16.840.1.101.3.4.1.46, aes-256-gcm, id-aes256-GCM } @ fips { 2.16.840.1.101.3.4.1.23, AES-192-OFB } @ fips { 2.16.840.1.101.3.4.1.7, aes-128-ccm, id-aes128-CCM } @ fips { 2.16.840.1.101.3.4.1.47, aes-256-ccm, id-aes256-CCM } @ fips { 2.16.840.1.101.3.4.1.45, AES-256-WRAP, AES256-WRAP, id-aes256-wrap } @ fips { 2.16.840.1.101.3.4.1.27, aes-192-ccm, id-aes192-CCM } @ fips { 1.3.111.2.1619.0.1.1, AES-128-XTS } @ fips { 2.16.840.1.101.3.4.1.5, AES-128-WRAP, AES128-WRAP, id-aes128-wrap } @ fips { 2.16.840.1.101.3.4.1.3, AES-128-OFB } @ fips { 2.16.840.1.101.3.4.1.1, AES-128-ECB } @ fips { 2.16.840.1.101.3.4.1.43, AES-256-OFB } @ fips { 2.16.840.1.101.3.4.1.21, AES-192-ECB } @ fips AES-128-CBC-CTS @ fips AES-192-CBC-CTS @ fips AES-256-CBC-CTS @ fips AES-256-CFB1 @ fips AES-192-CFB1 @ fips AES-128-CFB1 @ fips AES-256-CFB8 @ fips AES-192-CFB8 @ fips AES-128-CFB8 @ fips AES-256-CTR @ fips AES-192-CTR @ fips AES-128-CTR @ fips { AES-256-WRAP-INV, AES256-WRAP-INV } @ fips { AES-192-WRAP-INV, AES192-WRAP-INV } @ fips { AES-128-WRAP-INV, AES128-WRAP-INV } @ fips { AES-256-WRAP-PAD-INV, AES256-WRAP-PAD-INV } @ fips { AES-192-WRAP-PAD-INV, AES192-WRAP-PAD-INV } @ fips { AES-128-WRAP-PAD-INV, AES128-WRAP-PAD-INV } @ fips AES-128-CBC-HMAC-SHA1 @ fips AES-256-CBC-HMAC-SHA1 @ fips AES-128-CBC-HMAC-SHA256 @ fips AES-256-CBC-HMAC-SHA256 @ fips { DES-EDE3, DES-EDE3-ECB } @ fips { 1.2.840.113549.3.2, RC2, RC2-128, RC2-CBC } @ legacy { 1.2.840.113533.7.66.10, CAST, CAST-CBC, CAST5-CBC } @ legacy { 1.2.410.200004.1.3, SEED-ECB } @ legacy { 1.3.14.3.2.9, DES-CFB } @ legacy { 1.3.6.1.4.1.3029.1.2, BF, BF-CBC, BLOWFISH } @ legacy { 1.3.14.3.2.7, DES, DES-CBC } @ legacy { 1.3.14.3.2.6, DES-ECB } @ legacy { 1.2.840.113549.3.4, RC4 } @ legacy { 1.3.6.1.4.1.188.7.1.1.2, IDEA, IDEA-CBC } @ legacy { 1.2.410.200004.1.5, SEED-CFB, SEED-CFB128 } @

legacy { 1.3.14.3.2.8, DES-OFB } @ legacy { 1.2.410.200004.1.6, SEED-OFB, SEED-OFB128 } @ legacy { 1.2.410.200004.1.4, SEED, SEED-CBC } @ legacy CAST5-ECB @ legacy CAST5-OFB @ legacy CAST5-CFB @ legacy BF-ECB @ legacy BF-OFB @ legacy BF-CFB @ legacy IDEA-ECB @ legacy { IDEA-OFB, IDEA-OFB64 } @ legacy { IDEA-CFB, IDEA-CFB64 } @ legacy RC2-ECB @ legacy { RC2-40, RC2-40-CBC } @ legacy { RC2-64, RC2-64-CBC } @ legacy RC2-CFB @ legacy RC2-OFB @ legacy RC4-40 @ legacy RC4-HMAC-MD5 @ legacy { DESX, DESX-CBC } @ legacy DES-CFB1 @ legacy DES-CFB8 @ legacy

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 HKDF @ fips TLS13-KDF @ fips SSKDF @ fips { 1.2.840.113549.1.5.12, PBKDF2 } @ fips SSHKDF @ fips { X942KDF-CONCAT, X963KDF } @ fips TLS1-PRF @ fips KBKDF @ fips { X942KDF, X942KDF-ASN1 } @ fips PBKDF1 @ legacy PVKKDF @ legacy

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 CMAC @ fips { 1.0.9797.3.4, GMAC } @ fips HMAC @ fips { 2.16.840.1.101.3.4.2.19, KMAC-128, KMAC128 } @ fips { 2.16.840.1.101.3.4.2.20, KMAC-256, KMAC256 } @ fips

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 { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ fips { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2

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 { 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ fips { 1.3.101.110, X25519 } @ fips { 1.3.101.111, X448 } @ fips HKDF @ fips TLS1-PRF @ fips ECDH @ fips ECDH @ tpm2

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 { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ fips { 1.2.840.10040.4.1, 1.3.14.3.2.12, DSA, DSA-old, dsaEncryption, dsaEncryption-old } @ fips { 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 } @ fips { 1.3.101.112, ED25519 } @ fips { 1.3.101.113, ED448 } @ fips CMAC @ fips HMAC @ fips { 2.16.840.1.101.3.4.3.1, DSA-SHA2-224, DSA-SHA224, dsa_with_SHA224 } @ fips { 2.16.840.1.101.3.4.3.2, DSA-

SHA2-256, DSA-SHA256, dsa_with_SHA256 } @ fips { 1.2.840.1.101.3.4.3.3, DSA-SHA2-384, DSA-SHA384, dsa_with_SHA384, id-dsa-with-sha384 } @ fips { 1.2.840.1.101.3.4.3.4, DSA-SHA2-512, DSA-SHA512, dsa_with_SHA512, id-dsa-with-sha512 } @ fips { 2.16.840.1.101.3.4.3.5, DSA-SHA3-224, dsa_with_SHA3-224, id-dsa-with-sha3-224 } @ fips { 2.16.840.1.101.3.4.3.6, DSA-SHA3-256, dsa_with_SHA3-256, id-dsa-with-sha3-256 } @ fips { 2.16.840.1.101.3.4.3.7, DSA-SHA3-384, dsa_with_SHA3-384, id-dsa-with-sha3-384 } @ fips { 2.16.840.1.101.3.4.3.8, DSA-SHA3-512, dsa_with_SHA3-512, id-dsa-with-sha3-512 } @ fips { 1.2.840.113549.1.1.5, RSA-SHA-1, RSA-SHA1, sha1WithRSAEncryption } @ fips { 1.2.840.113549.1.1.14, RSA-SHA2-224, RSA-SHA224, sha224WithRSAEncryption } @ fips { 1.2.840.113549.1.1.11, RSA-SHA2-256, RSA-SHA256, sha256WithRSAEncryption } @ fips { 1.2.840.113549.1.1.12, RSA-SHA2-384, RSA-SHA384, sha384WithRSAEncryption } @ fips { 1.2.840.113549.1.1.13, RSA-SHA2-512, RSA-SHA512, sha512WithRSAEncryption } @ fips { 1.2.840.113549.1.1.15, RSA-SHA2-512/224, RSA-SHA512-224, sha512-224WithRSAEncryption } @ fips { 1.2.840.113549.1.1.16, RSA-SHA2-512/256, RSA-SHA512-256, sha512-256WithRSAEncryption } @ fips { 2.16.840.1.101.3.4.3.13, id-rsassa-pkcs1-v1_5-with-sha3-224, RSA-SHA3-224 } @ fips { 2.16.840.1.101.3.4.3.14, id-rsassa-pkcs1-v1_5-with-sha3-256, RSA-SHA3-256 } @ fips { 2.16.840.1.101.3.4.3.15, id-rsassa-pkcs1-v1_5-with-sha3-384, RSA-SHA3-384 } @ fips { 2.16.840.1.101.3.4.3.16, id-rsassa-pkcs1-v1_5-with-sha3-512, RSA-SHA3-512 } @ fips ED25519ph @ fips ED25519ctx @ fips ED448ph @ fips ECDSA @ fips { 1.2.840.10045.4.1, ECDSA-SHA-1, ECDSA-SHA1, ecdsa-with-SHA1 } @ fips { 1.2.840.10045.4.3.1, ECDSA-SHA2-224, ECDSA-SHA224, ecdsa-with-SHA224 } @ fips { 1.2.840.10045.4.3.2, ECDSA-SHA2-256, ECDSA-SHA256, ecdsa-with-SHA256 } @ fips { 1.2.840.10045.4.3.3, ECDSA-SHA2-384, ECDSA-SHA384, ecdsa-with-SHA384 } @ fips { 1.2.840.10045.4.3.4, ECDSA-SHA2-512, ECDSA-SHA512, ecdsa-with-SHA512 } @ fips { 2.16.840.1.101.3.4.3.9, ECDSA-SHA3-224, ecdsa_with_SHA3-224, id-ecdsa-with-sha3-224 } @ fips { 2.16.840.1.101.3.4.3.10, ECDSA-SHA3-256, ecdsa_with_SHA3-256, id-ecdsa-with-sha3-256 } @ fips { 2.16.840.1.101.3.4.3.11, ECDSA-SHA3-384, ecdsa_with_SHA3-384, id-ecdsa-with-sha3-384 } @ fips { 2.16.840.1.101.3.4.3.12, ECDSA-SHA3-512, ecdsa_with_SHA3-512, id-ecdsa-with-sha3-512 } @ fips dilithium2 @ oqsprovider p256_dilithium2 @ oqsprovider rsa3072_dilithium2 @ oqsprovider dilithium3 @ oqsprovider p384_dilithium3 @ oqsprovider dilithium5 @ oqsprovider p521_dilithium5 @ oqsprovider mldsa44 @ oqsprovider p256_mldsa44 @ oqsprovider rsa3072_mldsa44 @ oqsprovider mldsa44_pss2048 @ oqsprovider mldsa44_rsa2048 @ oqsprovider mldsa44_ed25519 @ oqsprovider mldsa44_p256 @ oqsprovider mldsa44_bp256 @ oqsprovider mldsa65 @ oqsprovider p384_mldsa65 @ oqsprovider mldsa65_pss3072 @ oqsprovider mldsa65_rsa3072 @ oqsprovider mldsa65_p256 @ oqsprovider mldsa65_bp256 @ oqsprovider mldsa65_ed25519 @ oqsprovider mldsa87 @ oqsprovider p521_mldsa87 @ oqsprovider mldsa87_p384 @ oqsprovider mldsa87_bp384 @ oqsprovider mldsa87_ed448 @ oqsprovider falcon512 @ oqsprovider p256_falcon512

@ oqsprovider rsa3072_falcon512 @ oqsprovider falconpadded512 @ oqsprovider p256_falconpadded512 @ oqsprovider rsa3072_falconpadded512 @ oqsprovider falcon1024 @ oqsprovider p521_falcon1024 @ oqsprovider falconpadded1024 @ oqsprovider p521_falconpadded1024 @ oqsprovider sphincssha2128fsimple @ oqsprovider p256_sphincssha2128fsimple @ oqsprovider rsa3072_sphincssha2128fsimple @ oqsprovider sphincssha2128ssimple @ oqsprovider p256_sphincssha2128ssimple @ oqsprovider rsa3072_sphincssha2128ssimple @ oqsprovider sphincssha2192fsimple @ oqsprovider p384_sphincssha2192fsimple @ oqsprovider sphincssha2192ssimple @ oqsprovider p384_sphincssha2192ssimple @ oqsprovider sphincssha2256fsimple @ oqsprovider p521_sphincssha2256fsimple @ oqsprovider sphincssha2256ssimple @ oqsprovider p521_sphincssha2256ssimple @ oqsprovider sphincsshake128fsimple @ oqsprovider p256_sphincsshake128fsimple @ oqsprovider rsa3072_sphincsshake128fsimple @ oqsprovider sphincsshake128ssimple @ oqsprovider p256_sphincsshake128ssimple @ oqsprovider rsa3072_sphincsshake128ssimple @ oqsprovider sphincsshake192fsimple @ oqsprovider p384_sphincsshake192fsimple @ oqsprovider sphincsshake192ssimple @ oqsprovider p384_sphincsshake192ssimple @ oqsprovider sphincsshake256fsimple @ oqsprovider p521_sphincsshake256fsimple @ oqsprovider sphincsshake256ssimple @ oqsprovider p521_sphincsshake256ssimple @ oqsprovider mayo1 @ oqsprovider p256_mayo1 @ oqsprovider mayo2 @ oqsprovider p256_mayo2 @ oqsprovider mayo3 @ oqsprovider p384_mayo3 @ oqsprovider mayo5 @ oqsprovider p521_mayo5 @ oqsprovider CROSSrsdp128balanced @ oqsprovider CROSSrsdp128fast @ oqsprovider CROSSrsdp128small @ oqsprovider CROSSrsdp192balanced @ oqsprovider CROSSrsdp192fast @ oqsprovider CROSSrsdp192small @ oqsprovider CROSSrsdp256small @ oqsprovider CROSSrsdpg128balanced @ oqsprovider CROSSrsdpg128fast @ oqsprovider CROSSrsdpg128small @ oqsprovider CROSSrsdpg192balanced @ oqsprovider CROSSrsdpg192fast @ oqsprovider CROSSrsdpg192small @ oqsprovider CROSSrsdpg256balanced @ oqsprovider CROSSrsdpg256fast @ oqsprovider CROSSrsdpg256small @ oqsprovider { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 ECDSA @ tpm2

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 { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ fips frodo640aes @ oqsprovider p256_frodo640aes @ oqsprovider x25519_frodo640aes @ oqsprovider frodo640shake @ oqsprovider p256_frodo640shake @ oqsprovider x25519_frodo640shake @ oqsprovider frodo976aes @ oqsprovider p384_frodo976aes @ oqsprovider x448_frodo976aes @ oqsprovider frodo976shake @ oqsprovider p384_frodo976shake @ oqsprovider x448_frodo976shake @ oqsprovider frodo1344aes @ oqsprovider p521_frodo1344aes @ oqsprovider frodo1344shake @ oqsprovider p521_frodo1344shake @ oqsprovider kyber512 @ oqsprovider p256_kyber512 @ oqsprovider x25519_kyber512 @ oqsprovider kyber768 @ oqsprovider p384_kyber768 @ oqsprovider x448_kyber768 @ oqsprovider x25519_kyber768 @ oqsprovider p256_kyber768 @ oqsprovider kyber1024 @ oqsprovider p521_kyber1024 @ oqsprovider mlkem512 @ oqsprovider p256_mlkem512 @ oqsprovider x25519_mlkem512 @ oqsprovider mlkem768 @ oqsprovider p384_mlkem768 @ oqsprovider x448_mlkem768 @ oqsprovider X25519MLKEM768 @ oqsprovider SecP256r1MLKEM768 @ oqsprovider mlkem1024 @ oqsprovider p521_mlkem1024 @ oqsprovider p384_mlkem1024 @ oqsprovider bikel1 @ oqsprovider p256_bikel1 @ oqsprovider x25519_bikel1 @ oqsprovider bikel3 @ oqsprovider p384_bikel3 @ oqsprovider x448_bikel3 @ oqsprovider bikel5 @ oqsprovider p521_bikel5 @ oqsprovider hqc128 @ oqsprovider p256_hqc128 @ oqsprovider x25519_hqc128 @ oqsprovider hqc192 @ oqsprovider p384_hqc192 @ oqsprovider x448_hqc192 @ oqsprovider hqc256 @ oqsprovider p521_hqc256 @ oqsprovider

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 Name: OpenSSL RSA implementation Type: Provider Algorithm IDs: { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ fips Name: OpenSSL PKCS#3 DH implementation Type: Provider Algorithm IDs: { 1.2.840.113549.1.3.1, DH, dhKeyAgreement } @ fips 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 } @ fips Name: OpenSSL EC implementation Type: Provider Algorithm IDs: { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ fips Name: OpenSSL RSA-PSS implementation Type: Provider Algorithm IDs: { 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ fips Name: OpenSSL X9.42 DH implementation Type: Provider Algorithm IDs: { 1.2.840.10046.2.1, dhpublicnumber, DHX, X9.42 DH } @ fips Name: OpenSSL X25519 implementation Type: Provider Algorithm IDs: { 1.3.101.110, X25519 } @ fips Name: OpenSSL X448 implementation Type: Provider Algorithm IDs: { 1.3.101.111, X448 } @ fips Name: OpenSSL ED25519 implementation Type: Provider Algorithm IDs: { 1.3.101.112, ED25519 } @ fips Name: OpenSSL ED448 implementation Type: Provider Algorithm IDs: { 1.3.101.113, ED448 } @ fips Name: OpenSSL HKDF via EVP_PKEY implementation Type: Provider Algorithm IDs: HKDF @ fips Name: OpenSSL TLS1_PRF via EVP_PKEY implementation Type: Provider Algorithm IDs: TLS1-PRF @ fips Name: OpenSSL CMAC via EVP_PKEY implementation Type: Provider Algorithm IDs: CMAC @ fips Name: OpenSSL HMAC via EVP_PKEY implementation Type: Provider Algorithm IDs: HMAC @ fips Name: dilithium2 Type: Provider Algorithm IDs: dilithium2 @ oqsprovider Name: p256_dilithium2 Type: Provider Algorithm IDs: p256_dilithium2 @ oqsprovider Name: rsa3072_dilithium2 Type: Provider Algorithm IDs: rsa3072_dilithium2 @ oqsprovider Name: dilithium3 Type: Provider Algorithm IDs: dilithium3 @ oqsprovider Name: p384_dilithium3 Type: Provider Algorithm IDs: p384_dilithium3 @ oqsprovider Name: dilithium5 Type: Provider Algorithm IDs: dilithium5 @ oqsprovider Name: p521_dilithium5 Type: Provider Algorithm IDs: p521_dilithium5 @ oqsprovider Name: mldsa44 Type: Provider Algorithm IDs: mldsa44 @ oqsprovider Name: p256_mldsa44 Type: Provider Algorithm IDs: p256_mldsa44 @ oqsprovider Name: rsa3072_mldsa44 Type: Provider Algorithm IDs: rsa3072_mldsa44 @ oqsprovider Name: mldsa44_pss2048 Type: Provider Algorithm IDs: mldsa44_pss2048 @ oqsprovider Name: mldsa44_rsa2048 Type: Provider Algorithm IDs: mldsa44_rsa2048 @ oqsprovider Name: mldsa44_ed25519 Type: Provider Algorithm IDs: mldsa44_ed25519 @ oqsprovider Name: mldsa44_p256 Type: Provider Algorithm IDs: mldsa44_p256 @ oqsprovider Name: mldsa44_bp256 Type: Provider Algorithm IDs: mldsa44_bp256 @ oqsprovider Name: mldsa65 Type: Provider Algorithm IDs: mldsa65 @ oqsprovider Name: p384_mldsa65 Type: Provider Algorithm IDs: p384_mldsa65 @ oqsprovider Name: mldsa65_pss3072 Type: Provider Algorithm IDs: mldsa65_pss3072 @ oqsprovider Name: mldsa65_rsa3072 Type: Provider Algorithm IDs: mldsa65_rsa3072 @ oqsprovider Name: mldsa65_p256 Type: Provider Algorithm IDs: mldsa65_p256 @ oqsprovider Name: mldsa65_bp256 Type: Provider Algorithm IDs: mldsa65_bp256 @ oqsprovider Name: mldsa65_ed25519 Type: Provider Algorithm IDs: mldsa65_ed25519 @ oqsprovider Name: mldsa87 Type: Provider Algorithm IDs: mldsa87 @ oqsprovider Name: p521_mldsa87 Type: Provider Algorithm IDs: p521_mldsa87 @ oqsprovider Name: mldsa87_p384 Type: Provider Algorithm IDs: mldsa87_p384 @ oqsprovider Name:

mldsa87_bp384 Type: Provider Algorithm IDs: mldsa87_bp384 @ oqsprovider Name: mldsa87_ed448 Type: Provider Algorithm IDs: mldsa87_ed448 @ oqsprovider Name: falcon512 Type: Provider Algorithm IDs: falcon512 @ oqsprovider Name: p256_falcon512 Type: Provider Algorithm IDs: p256_falcon512 @ oqsprovider Name: rsa3072_falcon512 Type: Provider Algorithm IDs: rsa3072_falcon512 @ oqsprovider Name: falconpadded512 Type: Provider Algorithm IDs: falconpadded512 @ oqsprovider Name: p256_falconpadded512 Type: Provider Algorithm IDs: p256_falconpadded512 @ oqsprovider Name: rsa3072_falconpadded512 Type: Provider Algorithm IDs: rsa3072_falconpadded512 @ oqsprovider Name: falcon1024 Type: Provider Algorithm IDs: falcon1024 @ oqsprovider Name: p521_falcon1024 Type: Provider Algorithm IDs: p521_falcon1024 @ oqsprovider Name: falconpadded1024 Type: Provider Algorithm IDs: falconpadded1024 @ oqsprovider Name: p521_falconpadded1024 Type: Provider Algorithm IDs: p521_falconpadded1024 @ oqsprovider Name: sphincssha2128fsimple Type: Provider Algorithm IDs: sphincssha2128fsimple @ oqsprovider Name: p256_sphincssha2128fsimple Type: Provider Algorithm IDs: p256_sphincssha2128fsimple @ oqsprovider Name: rsa3072_sphincssha2128fsimple Type: Provider Algorithm IDs: rsa3072_sphincssha2128fsimple @ oqsprovider Name: sphincssha2128ssimple Type: Provider Algorithm IDs: sphincssha2128ssimple @ oqsprovider Name: p256_sphincssha2128ssimple Type: Provider Algorithm IDs: p256_sphincssha2128ssimple @ oqsprovider Name: rsa3072_sphincssha2128ssimple Type: Provider Algorithm IDs: rsa3072_sphincssha2128ssimple @ oqsprovider Name: sphincssha2192fsimple Type: Provider Algorithm IDs: sphincssha2192fsimple @ oqsprovider Name: p384_sphincssha2192fsimple Type: Provider Algorithm IDs: p384_sphincssha2192fsimple @ oqsprovider Name: sphincssha2192ssimple Type: Provider Algorithm IDs: sphincssha2192ssimple @ oqsprovider Name: p384_sphincssha2192ssimple Type: Provider Algorithm IDs: p384_sphincssha2192ssimple @ oqsprovider Name: sphincssha2256fsimple Type: Provider Algorithm IDs: sphincssha2256fsimple @ oqsprovider Name: p521_sphincssha2256fsimple Type: Provider Algorithm IDs: p521_sphincssha2256fsimple @ oqsprovider Name: sphincssha2256ssimple Type: Provider Algorithm IDs: sphincssha2256ssimple @ oqsprovider Name: p521_sphincssha2256ssimple Type: Provider Algorithm IDs: p521_sphincssha2256ssimple @ oqsprovider Name: sphincsshake128fsimple Type: Provider Algorithm IDs: sphincsshake128fsimple @ oqsprovider Name: p256_sphincsshake128fsimple Type: Provider Algorithm IDs: p256_sphincsshake128fsimple @ oqsprovider Name: rsa3072_sphincsshake128fsimple Type: Provider Algorithm IDs: rsa3072_sphincsshake128fsimple @ oqsprovider Name: sphincsshake128ssimple Type: Provider Algorithm IDs: sphincsshake128ssimple @ oqsprovider Name: p256_sphincsshake128ssimple Type: Provider Algorithm IDs: p256_sphincsshake128ssimple @ oqsprovider Name: rsa3072_sphincsshake128ssimple Type: Provider Algorithm IDs: rsa3072_sphincsshake128ssimple @ oqsprovider Name: sphincsshake192fsimple Type: Provider Algorithm IDs: sphincsshake192fsimple @ oqsprovider Name: p384_sphincsshake192fsimple Type: Provider Algorithm IDs: p384_sphincsshake192fsimple @ oqsprovider Name: sphincsshake192ssimple Type: Provider Algorithm IDs: sphincsshake192ssimple @ oqsprovider Name: p384_sphincsshake192ssimple Type: Provider Algorithm IDs: p384_sphincsshake192ssimple @ oqsprovider Name: sphincsshake256fsimple Type: Provider Algorithm IDs: sphincsshake256fsimple @ oqsprovider Name: p521_sphincsshake256fsimple Type: Provider Algorithm IDs: p521_sphincsshake256fsimple @ oqsprovider Name: sphincsshake256ssimple Type: Provider Algorithm IDs: sphincsshake256ssimple @ oqsprovider Name: p521_sphincsshake256ssimple Type: Provider Algorithm IDs: p521_sphincsshake256ssimple @ oqsprovider Name: mayo1 Type: Provider Algorithm IDs: mayo1 @ oqsprovider Name: p256_mayo1 Type: Provider Algorithm IDs: p256_mayo1 @ oqsprovider Name: mayo2 Type: Provider Algorithm IDs: mayo2 @ oqsprovider Name: p256_mayo2 Type: Provider Algorithm IDs: p256_mayo2 @ oqsprovider Name: mayo3 Type: Provider Algorithm IDs: mayo3 @ oqsprovider Name: p384_mayo3 Type: Provider Algorithm IDs: p384_mayo3 @ oqsprovider Name: mayo5 Type: Provider Algorithm IDs: mayo5 @ oqsprovider Name: p521_mayo5 Type: Provider Algorithm IDs: p521_mayo5 @ oqsprovider Name: CROSSrsdp128balanced Type: Provider Algorithm IDs: CROSSrsdp128balanced @ oqsprovider Name: CROSSrsdp128fast Type: Provider Algorithm IDs: CROSSrsdp128fast @ oqsprovider Name: CROSSrsdp128small Type: Provider Algorithm IDs: CROSSrsdp128small @ oqsprovider Name: CROSSrsdp192balanced Type: Provider Algorithm IDs: CROSSrsdp192balanced @ oqsprovider Name: CROSSrsdp192fast Type: Provider Algorithm IDs: CROSSrsdp192fast @ oqsprovider Name: CROSSrsdp192small Type: Provider Algorithm IDs: CROSSrsdp192small @ oqsprovider Name: CROSSrsdp256small Type: Provider Algorithm IDs: CROSSrsdp256small @ oqsprovider Name: CROSSrsdpg128balanced Type: Provider Algorithm IDs: CROSSrsdpg128balanced @ oqsprovider Name: CROSSrsdpg128fast Type: Provider Algorithm IDs: CROSSrsdpg128fast @ oqsprovider Name: CROSSrsdpg128small Type: Provider Algorithm IDs: CROSSrsdpg128small @ oqsprovider Name: CROSSrsdpg192balanced Type: Provider Algorithm IDs: CROSSrsdpg192balanced @ oqsprovider Name: CROSSrsdpg192fast Type: Provider Algorithm IDs: CROSSrsdpg192fast @ oqsprovider Name: CROSSrsdpg192small Type: Provider Algorithm IDs: CROSSrsdpg192small @ oqsprovider Name: CROSSrsdpg256balanced Type: Provider Algorithm IDs: CROSSrsdpg256balanced @ oqsprovider Name: CROSSrsdpg256fast Type: Provider Algorithm IDs: CROSSrsdpg256fast @ oqsprovider Name: CROSSrsdpg256small Type: Provider Algorithm IDs: CROSSrsdpg256small @ oqsprovider Name: frodo640aes Type: Provider Algorithm IDs: frodo640aes @ oqsprovider Name: p256_frodo640aes Type: Provider Algorithm IDs: p256_frodo640aes @ oqsprovider Name: x25519_frodo640aes Type: Provider Algorithm IDs: x25519_frodo640aes @ oqsprovider Name: frodo640shake Type: Provider Algorithm IDs: frodo640shake @ oqsprovider Name: p256_frodo640shake Type: Provider Algorithm IDs: p256_frodo640shake @ oqsprovider Name: x25519_frodo640shake Type: Provider Algorithm IDs: x25519_frodo640shake @ oqsprovider Name: frodo976aes Type: Provider Algorithm IDs: frodo976aes @ oqsprovider Name: p384_frodo976aes Type: Provider Algorithm IDs: p384_frodo976aes @ oqsprovider Name: x448_frodo976aes Type: Provider Algorithm IDs: x448_frodo976aes @ oqsprovider Name: frodo976shake Type: Provider Algorithm IDs: frodo976shake @ oqsprovider Name: p384_frodo976shake Type: Provider Algorithm IDs: p384_frodo976shake @ oqsprovider Name: x448_frodo976shake Type: Provider Algorithm IDs: x448_frodo976shake @ oqsprovider Name: frodo1344aes Type: Provider Algorithm IDs: frodo1344aes @ oqsprovider Name: p521_frodo1344aes Type: Provider Algorithm IDs: p521_frodo1344aes @ oqsprovider Name: frodo1344shake Type: Provider Algorithm IDs: frodo1344shake @ oqsprovider Name: p521_frodo1344shake Type: Provider Algorithm IDs: p521_frodo1344shake @ oqsprovider Name: kyber512 Type: Provider Algorithm IDs: kyber512 @ oqsprovider Name: p256_kyber512 Type: Provider Algorithm IDs: p256_kyber512 @ oqsprovider Name: x25519_kyber512 Type: Provider Algorithm IDs: x25519_kyber512 @ oqsprovider Name: kyber768 Type: Provider Algorithm IDs: kyber768 @ oqsprovider Name: p384_kyber768 Type: Provider Algorithm IDs: p384_kyber768 @ oqsprovider Name: x448_kyber768 Type: Provider Algorithm IDs: x448_kyber768 @ oqsprovider Name: x25519_kyber768 Type: Provider Algorithm IDs: x25519_kyber768 @ oqsprovider Name: p256_kyber768 Type: Provider Algorithm IDs: p256_kyber768 @ oqsprovider Name: kyber1024 Type: Provider Algorithm IDs: kyber1024 @ oqsprovider Name: p521_kyber1024 Type: Provider Algorithm IDs: p521_kyber1024 @ oqsprovider Name: mlkem512 Type: Provider Algorithm IDs: mlkem512 @ oqsprovider Name: p256_mlkem512 Type: Provider Algorithm IDs: p256_mlkem512 @ oqsprovider Name: x25519_mlkem512 Type: Provider Algorithm IDs: x25519_mlkem512 @ oqsprovider Name: mlkem768 Type: Provider Algorithm IDs: mlkem768 @ oqsprovider Name: p384_mlkem768 Type: Provider Algorithm IDs: p384_mlkem768 @ oqsprovider Name: x448_mlkem768 Type: Provider Algorithm IDs: x448_mlkem768 @ oqsprovider Name: X25519MLKEM768 Type: Provider Algorithm IDs: X25519MLKEM768 @ oqsprovider Name: SecP256r1MLKEM768 Type: Provider Algorithm IDs: SecP256r1MLKEM768 @ oqsprovider Name: mlkem1024 Type: Provider Algorithm IDs: mlkem1024 @ oqsprovider Name: p521_mlkem1024 Type: Provider Algorithm IDs: p521_mlkem1024 @ oqsprovider Name: p384_mlkem1024 Type: Provider Algorithm IDs: p384_mlkem1024 @ oqsprovider Name: bikel1 Type: Provider Algorithm IDs: bikel1 @ oqsprovider Name: p256_bikel1 Type: Provider Algorithm IDs: p256_bikel1 @ oqsprovider Name: x25519_bikel1 Type: Provider Algorithm IDs: x25519_bikel1 @ oqsprovider Name: bikel3 Type: Provider Algorithm IDs: bikel3 @ oqsprovider Name: p384_bikel3 Type: Provider Algorithm IDs: p384_bikel3 @ oqsprovider Name: x448_bikel3 Type: Provider Algorithm IDs: x448_bikel3 @ oqsprovider Name: bikel5 Type: Provider Algorithm IDs: bikel5 @ oqsprovider Name: p521_bikel5 Type: Provider Algorithm IDs:

p521_bikel5 @ oqsprovider Name: hqc128 Type: Provider Algorithm IDs: hqc128 @ oqsprovider Name: p256_hqc128 Type: Provider Algorithm IDs: p256_hqc128 @ oqsprovider Name: x25519_hqc128 Type: Provider Algorithm IDs: x25519_hqc128 @ oqsprovider Name: hqc192 Type: Provider Algorithm IDs: hqc192 @ oqsprovider Name: p384_hqc192 Type: Provider Algorithm IDs: p384_hqc192 @ oqsprovider Name: x448_hqc192 Type: Provider Algorithm IDs: x448_hqc192 @ oqsprovider Name: hqc256 Type: Provider Algorithm IDs: hqc256 @ oqsprovider Name: p521_hqc256 Type: Provider Algorithm IDs: p521_hqc256 @ oqsprovider Name: PKCS11 RSA Implementation Type: Provider Algorithm IDs: { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ pkcs11 Name: PKCS11 EC Implementation Type: Provider Algorithm IDs: { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ pkcs11 Name: PKCS11 RSA PSS Implementation Type: Provider Algorithm IDs: { 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ pkcs11 Name: PKCS11 ED25519 Implementation Type: Provider Algorithm IDs: { 1.3.101.112, ED25519 } @ pkcs11 Name: PKCS11 ED448 Implementation Type: Provider Algorithm IDs: { 1.3.101.113, ED448 } @ pkcs11 Name: PKCS11 HKDF Implementation Type: Provider Algorithm IDs: HKDF @ pkcs11 Name: rsaEncryption Type: Provider Algorithm IDs: { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 Name: id-ecPublicKey Type: Provider Algorithm IDs: { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ tpm2 Name: RSASSA-PSS Type: Provider Algorithm IDs: { 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ tpm2

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 } @ default (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=EncryptedPrivateKeyI
{ 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
dilithium2 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
dilithium2 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
dilithium2 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
dilithium2 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
dilithium2 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
dilithium2 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
dilithium2 @ oqsprovider (provider=oqsprovider,output=text) p256_dilithium2
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_dilithium2 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_dilithium2 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p256_dilithium2 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p256_dilithium2 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p256_dilithium2 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p256_dilithium2 @ oqsprovider (provider=oqsprovider,output=text) rsa3072_dilithium2
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
rsa3072_dilithium2 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
rsa3072_dilithium2 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
rsa3072_dilithium2 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
rsa3072_dilithium2 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
rsa3072_dilithium2 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
rsa3072_dilithium2 @ oqsprovider (provider=oqsprovider,output=text)
dilithium3 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
dilithium3 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
```

```
dilithium3 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
dilithium3 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
dilithium3 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
dilithium3 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
dilithium3 @ oqsprovider (provider=oqsprovider,output=text) p384_dilithium3
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p384_dilithium3 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p384_dilithium3 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p384_dilithium3 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p384_dilithium3 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p384_dilithium3 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p384_dilithium3 @ oqsprovider (provider=oqsprovider,output=text) dilithium5
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
dilithium5 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
dilithium5 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
dilithium5 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
dilithium5 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
dilithium5 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
dilithium5 @ oqsprovider (provider=oqsprovider,output=text) p521_dilithium5
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p521_dilithium5 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p521_dilithium5 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p521_dilithium5 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p521_dilithium5 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p521_dilithium5 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p521_dilithium5 @ oqsprovider (provider=oqsprovider,output=text) mldsa44
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa44 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa44 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa44 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa44 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa44 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa44 @ oqsprovider (provider=oqsprovider,output=text) p256_mldsa44
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_mldsa44 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_mldsa44 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p256_mldsa44 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p256_mldsa44 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p256_mldsa44 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p256_mldsa44 @ oqsprovider (provider=oqsprovider,output=text) rsa3072_mldsa44
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
rsa3072_mldsa44 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
rsa3072_mldsa44 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
rsa3072_mldsa44 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
rsa3072_mldsa44 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
rsa3072_mldsa44 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
```

```
rsa3072_mldsa44 @ oqsprovider (provider=oqsprovider,output=text)
mldsa44_pss2048 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa44_pss2048 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa44_pss2048 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa44_pss2048 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa44_pss2048 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa44_pss2048 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa44_pss2048 @ oqsprovider (provider=oqsprovider,output=text)
mldsa44_rsa2048 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa44_rsa2048 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa44_rsa2048 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa44_rsa2048 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa44_rsa2048 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa44_rsa2048 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa44_rsa2048 @ oqsprovider (provider=oqsprovider,output=text)
mldsa44_ed25519 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa44_ed25519 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa44_ed25519 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa44_ed25519 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa44_ed25519 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa44_ed25519 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa44_ed25519 @ oqsprovider (provider=oqsprovider,output=text)
mldsa44_p256 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa44_p256 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa44_p256 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa44_p256 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa44_p256 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa44_p256 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa44_p256 @ oqsprovider (provider=oqsprovider,output=text) mldsa44_bp256
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa44_bp256 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa44_bp256 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa44_bp256 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa44_bp256 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa44_bp256 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa44_bp256 @ oqsprovider (provider=oqsprovider,output=text) mldsa65
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa65 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa65 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa65 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa65 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa65 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa65 @ oqsprovider (provider=oqsprovider,output=text) p384_mldsa65
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p384_mldsa65 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p384_mldsa65 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
```

p384_mldsa65 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p384_mldsa65 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p384_mldsa65 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p384_mldsa65 @ oqsprovider (provider=oqsprovider,output=text) mldsa65_pss3072
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa65_pss3072 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa65_pss3072 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa65_pss3072 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa65_pss3072 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa65_pss3072 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa65_pss3072 @ oqsprovider (provider=oqsprovider,output=text)
mldsa65_rsa3072 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa65_rsa3072 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa65_rsa3072 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa65_rsa3072 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa65_rsa3072 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa65_rsa3072 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa65_rsa3072 @ oqsprovider (provider=oqsprovider,output=text)
mldsa65_p256 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa65_p256 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa65_p256 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa65_p256 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa65_p256 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa65_p256 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa65_p256 @ oqsprovider (provider=oqsprovider,output=text) mldsa65_bp256
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa65_bp256 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa65_bp256 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa65_bp256 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa65_bp256 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa65_bp256 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa65_bp256 @ oqsprovider (provider=oqsprovider,output=text) mldsa65_ed25519
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa65_ed25519 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa65_ed25519 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa65_ed25519 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa65_ed25519 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa65_ed25519 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa65_ed25519 @ oqsprovider (provider=oqsprovider,output=text) mldsa87
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa87 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa87 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa87 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa87 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa87 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa87 @ oqsprovider (provider=oqsprovider,output=text) p521_mldsa87

```
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p521_mldsa87 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p521_mldsa87 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p521_mldsa87 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p521_mldsa87 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p521_mldsa87 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p521_mldsa87 @ oqsprovider (provider=oqsprovider,output=text) mldsa87_p384
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa87_p384 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa87_p384 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa87_p384 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa87_p384 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa87_p384 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa87_p384 @ oqsprovider (provider=oqsprovider,output=text) mldsa87_bp384
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa87_bp384 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa87_bp384 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa87_bp384 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa87_bp384 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa87_bp384 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa87_bp384 @ oqsprovider (provider=oqsprovider,output=text) mldsa87_ed448
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mldsa87_ed448 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mldsa87_ed448 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mldsa87_ed448 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mldsa87_ed448 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mldsa87_ed448 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mldsa87_ed448 @ oqsprovider (provider=oqsprovider,output=text) falcon512
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
falcon512 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
falcon512 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
falcon512 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
falcon512 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
falcon512 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
falcon512 @ oqsprovider (provider=oqsprovider,output=text) p256_falcon512
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_falcon512 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_falcon512 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p256_falcon512 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p256_falcon512 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p256_falcon512 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p256_falcon512 @ oqsprovider (provider=oqsprovider,output=text) rsa3072_falcon512
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
rsa3072_falcon512 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
rsa3072_falcon512 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
rsa3072_falcon512 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
```

rsa3072_falcon512 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
rsa3072_falcon512 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
rsa3072_falcon512 @ oqsprovider (provider=oqsprovider,output=text) falconpadded512 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
falconpadded512 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
falconpadded512 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
falconpadded512 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
falconpadded512 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
falconpadded512 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
falconpadded512 @ oqsprovider (provider=oqsprovider,output=text) p256_falconpadded512
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_falconpadded512 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_falconpadded512 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo
p256_falconpadded512 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInf
p256_falconpadded512 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p256_falconpadded512 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p256_falconpadded512 @ oqsprovider (provider=oqsprovider,output=text)
rsa3072_falconpadded512 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
rsa3072_falconpadded512 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
rsa3072_falconpadded512 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyI
rsa3072_falconpadded512 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKey
rsa3072_falconpadded512 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
rsa3072_falconpadded512 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo
rsa3072_falconpadded512 @ oqsprovider (provider=oqsprovider,output=text)
falcon1024 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
falcon1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
falcon1024 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
falcon1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
falcon1024 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
falcon1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
falcon1024 @ oqsprovider (provider=oqsprovider,output=text) p521_falcon1024
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p521_falcon1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p521_falcon1024 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p521_falcon1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p521_falcon1024 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p521_falcon1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p521_falcon1024 @ oqsprovider (provider=oqsprovider,output=text) falconpadded1024 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
falconpadded1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
falconpadded1024 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
falconpadded1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
falconpadded1024 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
falconpadded1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
falconpadded1024 @ oqsprovider (provider=oqsprovider,output=text)
p521_falconpadded1024 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)

```
p521_falconpadded1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p521_falconpadded1024 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInf
p521_falconpadded1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyIn
p521_falconpadded1024 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p521_falconpadded1024 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p521_falconpadded1024 @ oqsprovider (provider=oqsprovider,output=text)
sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo
sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=text)
p256_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKe
p256_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateK
p256_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyIn
p256_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyI
p256_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=text)
rsa3072_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
rsa3072_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
rsa3072_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivate
rsa3072_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivat
rsa3072_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKey
rsa3072_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKe
rsa3072_sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,output=text)
sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo
sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=text)
p256_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKe
p256_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateK
p256_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyIn
p256_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyI
p256_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=text)
rsa3072_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
rsa3072_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
rsa3072_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivate
rsa3072_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivat
rsa3072_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKey
rsa3072_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicK
rsa3072_sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,output=text)
sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo
sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=text)
p384_sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p384_sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p384_sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKe
p384_sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateK
p384_sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyIn
p384_sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyI
p384_sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,output=text)
sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo
sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=text)
p384_sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p384_sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p384_sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKe
p384_sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateK
p384_sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyIn
p384_sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyI
p384_sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,output=text)
sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo
sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=text)
p521_sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p521_sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p521_sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKe
p521_sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateK
p521_sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyIn
p521_sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyI
p521_sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,output=text)
sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
```

```
sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo
sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=text)
p521_sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p521_sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p521_sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKe
p521_sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateK
p521_sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyIn
p521_sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyI
p521_sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,output=text)
sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo
sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInf
sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=text)
p256_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateK
p256_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivate
p256_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyI
p256_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKey
p256_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=text)
rsa3072_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
rsa3072_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo
rsa3072_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivat
rsa3072_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPriva
rsa3072_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKe
rsa3072_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicK
rsa3072_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,output=text)
sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo
sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInf
sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=text)
p256_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateK
p256_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivate
p256_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyI
p256_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKey
p256_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=text)
rsa3072_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
rsa3072_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo
rsa3072_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPriva
rsa3072_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPriva
rsa3072_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicK
rsa3072_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicK
rsa3072_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,output=text)
sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo
sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInf
sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=text)
p384_sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p384_sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p384_sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateK
p384_sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivate
p384_sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyI
p384_sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKey
p384_sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,output=text)
sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo
sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInf
sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=text)
p384_sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p384_sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p384_sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateK
p384_sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivate
p384_sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyI
p384_sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKey
p384_sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,output=text)
sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo
sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInf
sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=text)
p521_sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p521_sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p521_sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateK
```

p521_sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivate
p521_sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyI
p521_sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKey
p521_sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,output=text)
sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo
sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInf
sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=text)
p521_sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p521_sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p521_sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateK
p521_sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivate
p521_sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyI
p521_sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKey
p521_sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,output=text)
mayo1 @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mayo1 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mayo1 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mayo1 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mayo1 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mayo1 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mayo1 @ oqsprovider (provider=oqsprovider,output=text) p256_mayo1 @
oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_mayo1 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_mayo1 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p256_mayo1 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p256_mayo1 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p256_mayo1 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p256_mayo1 @ oqsprovider (provider=oqsprovider,output=text) mayo2 @
oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mayo2 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mayo2 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mayo2 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mayo2 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mayo2 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mayo2 @ oqsprovider (provider=oqsprovider,output=text) p256_mayo2 @
oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p256_mayo2 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p256_mayo2 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p256_mayo2 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p256_mayo2 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p256_mayo2 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p256_mayo2 @ oqsprovider (provider=oqsprovider,output=text) mayo3 @

```
oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mayo3 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mayo3 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mayo3 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mayo3 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mayo3 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mayo3 @ oqsprovider (provider=oqsprovider,output=text) p384_mayo3 @
oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p384_mayo3 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p384_mayo3 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p384_mayo3 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p384_mayo3 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p384_mayo3 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p384_mayo3 @ oqsprovider (provider=oqsprovider,output=text) mayo5 @
oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
mayo5 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
mayo5 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
mayo5 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
mayo5 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
mayo5 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
mayo5 @ oqsprovider (provider=oqsprovider,output=text) p521_mayo5 @
oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
p521_mayo5 @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
p521_mayo5 @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
p521_mayo5 @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
p521_mayo5 @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
p521_mayo5 @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
p521_mayo5 @ oqsprovider (provider=oqsprovider,output=text) CROSSrsdp128balanced
@ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
CROSSrsdp128balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdp128balanced @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInf
CROSSrsdp128balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyIn
CROSSrsdp128balanced @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
CROSSrsdp128balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
CROSSrsdp128balanced @ oqsprovider (provider=oqsprovider,output=text)
CROSSrsdp128fast @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
CROSSrsdp128fast @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdp128fast @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
CROSSrsdp128fast @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
CROSSrsdp128fast @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
CROSSrsdp128fast @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
CROSSrsdp128fast @ oqsprovider (provider=oqsprovider,output=text)
CROSSrsdp128small @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
CROSSrsdp128small @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdp128small @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
CROSSrsdp128small @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
```

CROSSrsdp128small @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)

CROSSrsdp128small @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)

CROSSrsdp128small @ oqsprovider (provider=oqsprovider,output=text)

CROSSrsdp192balanced @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)

CROSSrsdp192balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)

CROSSrsdp192balanced @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInf

CROSSrsdp192balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyIn

CROSSrsdp192balanced @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)

CROSSrsdp192balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)

CROSSrsdp192balanced @ oqsprovider (provider=oqsprovider,output=text)

CROSSrsdp192fast @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)

CROSSrsdp192fast @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)

CROSSrsdp192fast @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)

CROSSrsdp192fast @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)

CROSSrsdp192fast @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)

CROSSrsdp192fast @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)

CROSSrsdp192fast @ oqsprovider (provider=oqsprovider,output=text)

CROSSrsdp192small @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)

CROSSrsdp192small @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)

CROSSrsdp192small @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)

CROSSrsdp192small @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)

CROSSrsdp192small @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)

CROSSrsdp192small @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)

CROSSrsdp192small @ oqsprovider (provider=oqsprovider,output=text)

CROSSrsdp256small @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)

CROSSrsdp256small @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)

CROSSrsdp256small @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)

CROSSrsdp256small @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)

CROSSrsdp256small @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)

CROSSrsdp256small @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)

CROSSrsdp256small @ oqsprovider (provider=oqsprovider,output=text)

CROSSrsdpg128balanced @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)

CROSSrsdpg128balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)

CROSSrsdpg128balanced @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyIn

CROSSrsdpg128balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyI

CROSSrsdpg128balanced @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)

CROSSrsdpg128balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)

CROSSrsdpg128balanced @ oqsprovider (provider=oqsprovider,output=text)

CROSSrsdpg128fast @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)

CROSSrsdpg128fast @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)

CROSSrsdpg128fast @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)

CROSSrsdpg128fast @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)

CROSSrsdpg128fast @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)

CROSSrsdpg128fast @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)

CROSSrsdpg128fast @ oqsprovider (provider=oqsprovider,output=text)

CROSSrsdpg128small @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)

```
CROSSrsdpg128small @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdpg128small @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg128small @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg128small @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg128small @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
CROSSrsdpg128small @ oqsprovider (provider=oqsprovider,output=text)
CROSSrsdpg192balanced @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
CROSSrsdpg192balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdpg192balanced @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyIn
CROSSrsdpg192balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyI
CROSSrsdpg192balanced @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg192balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
CROSSrsdpg192balanced @ oqsprovider (provider=oqsprovider,output=text)
CROSSrsdpg192fast @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
CROSSrsdpg192fast @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdpg192fast @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg192fast @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg192fast @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg192fast @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
CROSSrsdpg192fast @ oqsprovider (provider=oqsprovider,output=text)
CROSSrsdpg192small @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
CROSSrsdpg192small @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdpg192small @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg192small @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg192small @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg192small @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
CROSSrsdpg192small @ oqsprovider (provider=oqsprovider,output=text)
CROSSrsdpg256balanced @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
CROSSrsdpg256balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdpg256balanced @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyIn
CROSSrsdpg256balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyI
CROSSrsdpg256balanced @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg256balanced @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
CROSSrsdpg256balanced @ oqsprovider (provider=oqsprovider,output=text)
CROSSrsdpg256fast @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
CROSSrsdpg256fast @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdpg256fast @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg256fast @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg256fast @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg256fast @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
CROSSrsdpg256fast @ oqsprovider (provider=oqsprovider,output=text)
CROSSrsdpg256small @ oqsprovider (provider=oqsprovider,output=der,structure=PrivateKeyInfo)
CROSSrsdpg256small @ oqsprovider (provider=oqsprovider,output=pem,structure=PrivateKeyInfo)
CROSSrsdpg256small @ oqsprovider (provider=oqsprovider,output=der,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg256small @ oqsprovider (provider=oqsprovider,output=pem,structure=EncryptedPrivateKeyInfo)
CROSSrsdpg256small @ oqsprovider (provider=oqsprovider,output=der,structure=SubjectPublicKeyInfo)
```

```
CROSSrsdpg256small @ oqsprovider (provider=oqsprovider,output=pem,structure=SubjectPublicKeyInfo)
CROSSrsdpg256small @ oqsprovider (provider=oqsprovider,output=text) {
1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 (provider=tpm2,output=der,structure=PrivateKe
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 (provider=tpm2,output=pem,structure=Private
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 (provider=tpm2,output=der,structure=pkcs1)
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 (provider=tpm2,output=pem,structure=pkcs1)
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 (provider=tpm2,output=der,structure=Subject
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 (provider=tpm2,output=pem,structure=Subject
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 (provider=tpm2,output=text)
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ tpm2 (provider=tpm2,output=der,structure=PrivateKeyInfo)
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ tpm2 (provider=tpm2,output=pem,structure=PrivateKeyInfo)
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ tpm2 (provider=tpm2,output=der,structure=SubjectPublicKeyInf
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ tpm2 (provider=tpm2,output=pem,structure=SubjectPublicKeyIn
{ 1.2.840.10045.2.1, EC, id-ecPublicKey } @ tpm2 (provider=tpm2,output=text)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ tpm2
(provider=tpm2,output=der,structure=PrivateKeyInfo) { 1.2.840.113549.1.1.10,
RSA-PSS, RSASSA-PSS, rsassaPss } @ tpm2 (provider=tpm2,output=pem,structure=PrivateKeyInfo)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ tpm2
(provider=tpm2,output=der,structure=pkcs1) { 1.2.840.113549.1.1.10, RSA-PSS,
RSASSA-PSS, rsassaPss } @ tpm2 (provider=tpm2,output=pem,structure=pkcs1)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ tpm2
(provider=tpm2,output=der,structure=SubjectPublicKeyInfo) { 1.2.840.113549.1.1.10,
RSA-PSS, RSASSA-PSS, rsassaPss } @ tpm2 (provider=tpm2,output=pem,structure=SubjectPublicKeyInfo)
{ 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ tpm2
(provider=tpm2,output=text)
```

```
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)
dilithium2 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
dilithium2 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256_dilithium2 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256_dilithium2 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
rsa3072_dilithium2 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
rsa3072_dilithium2 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
dilithium3 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
dilithium3 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p384_dilithium3 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p384_dilithium3 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
dilithium5 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
dilithium5 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p521_dilithium5 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p521_dilithium5 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa44 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)

```
mldsa44 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256_mldsa44 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256_mldsa44 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
rsa3072_mldsa44 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
rsa3072_mldsa44 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa44_pss2048 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa44_pss2048 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa44_rsa2048 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa44_rsa2048 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa44_ed25519 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa44_ed25519 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa44_p256 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa44_p256 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa44_bp256 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa44_bp256 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa65 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa65 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p384_mldsa65 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p384_mldsa65 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa65_pss3072 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa65_pss3072 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa65_rsa3072 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa65_rsa3072 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa65_p256 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa65_p256 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa65_bp256 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa65_bp256 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa65_ed25519 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa65_ed25519 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa87 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa87 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p521_mldsa87 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p521_mldsa87 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa87_p384 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa87_p384 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa87_bp384 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa87_bp384 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mldsa87_ed448 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mldsa87_ed448 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
falcon512 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
falcon512 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256_falcon512 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256_falcon512 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
rsa3072_falcon512 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
rsa3072_falcon512 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
falconpadded512 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
```

```
falconpadded512 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256__falconpadded512 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256__falconpadded512 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
rsa3072__falconpadded512 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
rsa3072__falconpadded512 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
falcon1024 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
falcon1024 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p521__falcon1024 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p521__falcon1024 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
falconpadded1024 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
falconpadded1024 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p521__falconpadded1024 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p521__falconpadded1024 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256__sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256__sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo
rsa3072__sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
rsa3072__sphincssha2128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyI
sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256__sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256__sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo
rsa3072__sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
rsa3072__sphincssha2128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyI
sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p384__sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p384__sphincssha2192fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo
sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p384__sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p384__sphincssha2192ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo
sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p521__sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p521__sphincssha2256fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo
sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p521__sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p521__sphincssha2256ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo
sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256__sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256__sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInf
rsa3072__sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
```

```
rsa3072_sphincsshake128fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKey
sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyIn
rsa3072_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
rsa3072_sphincsshake128ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKey
sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p384_sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p384_sphincsshake192fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInf
sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p384_sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p384_sphincsshake192ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyIn
sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p521_sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p521_sphincsshake256fsimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInf
sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p521_sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p521_sphincsshake256ssimple @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyIn
mayo1 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mayo1 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256_mayo1 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256_mayo1 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mayo2 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mayo2 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p256_mayo2 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p256_mayo2 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mayo3 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mayo3 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p384_mayo3 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p384_mayo3 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
mayo5 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
mayo5 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
p521_mayo5 @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
p521_mayo5 @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdp128balanced @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdp128balanced @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdp128fast @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdp128fast @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdp128small @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdp128small @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdp192balanced @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
```

```
CROSSrsdp192balanced @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdp192fast @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdp192fast @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdp192small @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdp192small @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdp256small @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdp256small @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg128balanced @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdpg128balanced @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg128fast @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdpg128fast @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg128small @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdpg128small @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg192balanced @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdpg192balanced @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg192fast @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdpg192fast @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg192small @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdpg192small @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg256balanced @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdpg256balanced @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg256fast @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdpg256fast @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
CROSSrsdpg256small @ oqsprovider (provider=oqsprovider,input=der,structure=PrivateKeyInfo)
CROSSrsdpg256small @ oqsprovider (provider=oqsprovider,input=der,structure=SubjectPublicKeyInfo)
{ 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ pkcs11 (provider=pkcs11,input=der,structure=pk11-uri) { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ pkcs11 (provider=pkcs11,input=der,structure=pk11-uri) { 1.2.840.113549.1.1.10, RSA-PSS, RSASSA-PSS, rsassaPss } @ pkcs11 (provider=pkcs11,input=der,structure=pk11-uri) { 1.3.101.112, ED25519 } @ pkcs11 (provider=pkcs11,input=der,structure=pk11-uri) { 1.3.101.113, ED448 } @ pkcs11 (provider=pkcs11,input=der,structure=pk11-uri) DER @ pkcs11 (provider=pkcs11,input=pem) { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ tpm2 (provider=tpm2,input=der,structure=TSS2) { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ tpm2 (provider=tpm2,input=der,structure=TSS2) DER @ tpm2 (provider=tpm2,input=pem)
```

Provided STORE LOADERs: file @ default pkcs11 @ pkcs11 object @ tpm2 handle @ tpm2