

NXP JCOP 4.1 V2.2.1

Card ATR: 3B:FA:18:00:00:81:31:FE:45:4A:43:4F:50:34:31:56:32:32:31:9D

Note: Card is probably without garbage collector - it is not possible to test all supported algorithms at once. When certain number of instances is allocated, further instances cannot be obtained, even when supported by card. Re-installation of whole applet is necessary.

Note: Unclear situation with AES support - AES Cipher object can be obtained, but not AESKey object. According to forums posts, AES is available in hardware, but is usually disabled (and cannot be re-enabled).

| javacardx.crypto.Cipher | supported | time |
|----------------------------------|------------------|-------------|
| ALG_DES_CBC_NOPAD | yes | |
| ALG_DES_CBC_ISO9797_M1 | yes | |
| ALG_DES_CBC_ISO9797_M2 | yes | |
| ALG_DES_CBC_PKCS5 | no | |
| ALG_DES_ECB_NOPAD | yes | |
| ALG_DES_ECB_ISO9797_M1 | yes | |
| ALG_DES_ECB_ISO9797_M2 | yes | |
| ALG_DES_ECB_PKCS5 | no | |
| ALG_RSA_ISO14888 | no | |
| ALG_RSA_PKCS1 | yes | |
| ALG_RSA_ISO9796 | no | |
| ALG_RSA_NOPAD | yes | |
| ALG_AES_BLOCK_128_CBC_NOPAD | yes | |
| ALG_AES_BLOCK_128_ECB_NOPAD | yes | |
| ALG_RSA_PKCS1_OAEP | no | |
| ALG_KOREAN_SEED_ECB_NOPAD | no | |
| ALG_KOREAN_SEED_CBC_NOPAD | no | |
| javacard.crypto.Signature | | |
| ALG_DES_MAC4_NOPAD | no | |
| ALG_DES_MAC8_NOPAD | yes | |
| ALG_DES_MAC4_ISO9797_M1 | no | |
| ALG_DES_MAC8_ISO9797_M1 | yes | |
| ALG_DES_MAC4_ISO9797_M2 | no | |
| ALG_DES_MAC8_ISO9797_M2 | yes | |
| ALG_DES_MAC4_PKCS5 | no | |
| ALG_DES_MAC8_PKCS5 | no | |
| ALG_RSA_SHA_ISO9796 | yes | |
| ALG_RSA_SHA_PKCS1 | yes | |
| ALG_RSA_MD5_PKCS1 | yes | |
| ALG_RSA_RIPEMD160_ISO9796 | no | |
| ALG_RSA_RIPEMD160_PKCS1 | no | |
| ALG_DSA_SHA | no | |
| ALG_RSA_SHA_RFC2409 | no | |
| ALG_RSA_MD5_RFC2409 | no | |
| ALG_ECDSA_SHA | yes | |
| ALG_AES_MAC_128_NOPAD | yes | |
| ALG_DES_MAC4_ISO9797_1_M2_ALG3 | no | |
| ALG_DES_MAC8_ISO9797_1_M2_ALG3 | yes | |
| ALG_RSA_SHA_PKCS1_PSS | no | |

| | | |
|--|-----|--|
| ALG_RSA_MD5_PKCS1_PSS | no | |
| ALG_RSA_RIPEMD160_PKCS1_PSS | no | |
| ALG_HMAC_SHA1 | no | |
| ALG_HMAC_SHA_256 | no | |
| ALG_HMAC_SHA_384 | no | |
| ALG_HMAC_SHA_512 | no | |
| ALG_HMAC_MD5 | no | |
| ALG_HMAC_RIPEMD160 | no | |
| ALG_RSA_SHA_ISO9796_MR | no | |
| ALG_RSA_RIPEMD160_ISO9796_MR | no | |
| ALG_SEED_MAC_NOPAD | no | |
| javacard.security.MessageDigest | | |
| ALG_SHA | yes | |
| ALG_MD5 | yes | |
| ALG_RIPEMD160 | no | |
| ALG_SHA_256 | no | |
| ALG_SHA_384 | no | |
| ALG_SHA_512 | no | |
| javacard.security.RandomData | | |
| ALG_PSEUDO_RANDOM | yes | |
| ALG_SECURE_RANDOM | yes | |
| javacard.security.KeyBuilder | | |
| TYPE_DES_TRANSIENT_RESET | yes | |
| TYPE_DES_TRANSIENT_DESELECT | yes | |
| TYPE_DES_LENGTH_DES | yes | |
| TYPE_DES_LENGTH_DES3_2KEY | yes | |
| TYPE_DES_LENGTH_DES3_3KEY | yes | |
| TYPE_AES_TRANSIENT_RESET | no | |
| TYPE_AES_TRANSIENT_DESELECT | no | |
| TYPE_AES_LENGTH_AES_128 | no | |
| TYPE_AES_LENGTH_AES_192 | no | |
| TYPE_AES_LENGTH_AES_256 | no | |
| TYPE_RSA_PUBLIC_LENGTH_RSA_512 | yes | |
| TYPE_RSA_PUBLIC_LENGTH_RSA_736 | yes | |
| TYPE_RSA_PUBLIC_LENGTH_RSA_768 | yes | |
| TYPE_RSA_PUBLIC_LENGTH_RSA_896 | yes | |
| TYPE_RSA_PUBLIC_LENGTH_RSA_1024 | yes | |
| TYPE_RSA_PUBLIC_LENGTH_RSA_1280 | yes | |
| TYPE_RSA_PUBLIC_LENGTH_RSA_1536 | yes | |
| TYPE_RSA_PUBLIC_LENGTH_RSA_1984 | yes | |
| TYPE_RSA_PUBLIC_LENGTH_RSA_2048 | yes | |
| TYPE_RSA_PRIVATE_LENGTH_RSA_512 | yes | |
| TYPE_RSA_PRIVATE_LENGTH_RSA_736 | yes | |
| TYPE_RSA_PRIVATE_LENGTH_RSA_768 | yes | |
| TYPE_RSA_PRIVATE_LENGTH_RSA_896 | yes | |
| TYPE_RSA_PRIVATE_LENGTH_RSA_1024 | yes | |
| TYPE_RSA_PRIVATE_LENGTH_RSA_1280 | yes | |
| TYPE_RSA_PRIVATE_LENGTH_RSA_1536 | yes | |
| TYPE_RSA_PRIVATE_LENGTH_RSA_1984 | yes | |
| TYPE_RSA_PRIVATE_LENGTH_RSA_2048 | yes | |
| TYPE_RSA_CRT_PRIVATE_LENGTH_RSA_512 | yes | |
| TYPE_RSA_CRT_PRIVATE_LENGTH_RSA_736 | no | |

| | | |
|---|-----|--------|
| TYPE_RSA_CRT_PRIVATE_LENGTH_RSA_768 | yes | |
| TYPE_RSA_CRT_PRIVATE_LENGTH_RSA_896 | yes | |
| TYPE_RSA_CRT_PRIVATE_LENGTH_RSA_1024 | yes | |
| TYPE_RSA_CRT_PRIVATE_LENGTH_RSA_1280 | yes | |
| TYPE_RSA_CRT_PRIVATE_LENGTH_RSA_1536 | yes | |
| TYPE_RSA_CRT_PRIVATE_LENGTH_RSA_1984 | yes | |
| TYPE_RSA_CRT_PRIVATE_LENGTH_RSA_2048 | yes | |
| TYPE_DSA_PRIVATE_LENGTH_DSA_512 | no | |
| TYPE_DSA_PRIVATE_LENGTH_DSA_768 | no | |
| TYPE_DSA_PRIVATE_LENGTH_DSA_1024 | no | |
| TYPE_DSA_PUBLIC_LENGTH_DSA_512 | no | |
| TYPE_DSA_PUBLIC_LENGTH_DSA_768 | no | |
| TYPE_DSA_PUBLIC_LENGTH_DSA_1024 | no | |
| TYPE_EC_F2M_PRIVATE_LENGTH_EC_F2M_113 | yes | |
| TYPE_EC_F2M_PRIVATE_LENGTH_EC_F2M_131 | yes | |
| TYPE_EC_F2M_PRIVATE_LENGTH_EC_F2M_163 | yes | |
| TYPE_EC_F2M_PRIVATE_LENGTH_EC_F2M_193 | yes | |
| TYPE_EC_FP_PRIVATE_LENGTH_EC_FP_112 | no | |
| TYPE_EC_FP_PRIVATE_LENGTH_EC_FP_128 | no | |
| TYPE_EC_FP_PRIVATE_LENGTH_EC_FP_160 | no | |
| TYPE_EC_FP_PRIVATE_LENGTH_EC_FP_192 | no | |
| TYPE_KOREAN_SEED_TRANSIENT_RESET | no | |
| TYPE_KOREAN_SEED_TRANSIENT_DESELECT | no | |
| TYPE_KOREAN_SEED_LENGTH_KOREAN_SEED_128 | no | |
| TYPE_HMAC_TRANSIENT_RESET | no | |
| TYPE_HMAC_TRANSIENT_DESELECT | no | |
| TYPE_HMAC_LENGTH_HMAC_SHA_1_BLOCK_64 | no | |
| TYPE_HMAC_LENGTH_HMAC_SHA_256_BLOCK_64 | no | |
| TYPE_HMAC_LENGTH_HMAC_SHA_384_BLOCK_64 | no | |
| TYPE_HMAC_LENGTH_HMAC_SHA_512_BLOCK_64 | no | |
| javacard.security.KeyPair ALG_RSA on-card generation | | |
| ALG_RSA_LENGTH_RSA_512 | no | |
| ALG_RSA_LENGTH_RSA_736 | no | |
| ALG_RSA_LENGTH_RSA_768 | no | |
| ALG_RSA_LENGTH_RSA_896 | no | |
| ALG_RSA_LENGTH_RSA_1024 | no | |
| ALG_RSA_LENGTH_RSA_1280 | no | |
| ALG_RSA_LENGTH_RSA_1536 | no | |
| ALG_RSA_LENGTH_RSA_1984 | no | |
| ALG_RSA_LENGTH_RSA_2048 | no | |
| javacard.security.KeyPair ALG_RSA_CRT on-card generation | | |
| ALG_RSA_CRT_LENGTH_RSA_512 | yes | 0.531 |
| ALG_RSA_CRT_LENGTH_RSA_736 | no | |
| ALG_RSA_CRT_LENGTH_RSA_768 | yes | 0.859 |
| ALG_RSA_CRT_LENGTH_RSA_896 | yes | 2.281 |
| ALG_RSA_CRT_LENGTH_RSA_1024 | yes | 2.422 |
| ALG_RSA_CRT_LENGTH_RSA_1280 | yes | 3.266 |
| ALG_RSA_CRT_LENGTH_RSA_1536 | yes | 17.953 |
| javacard.security.KeyPair ALG_DSA on-card generation | | |
| ALG_DSA_LENGTH_DSA_512 | no | |
| ALG_DSA_LENGTH_DSA_768 | no | |

| | | |
|--|-----|-------|
| ALG_DSA LENGTH_DSA_1024 | no | |
| javacard.security.KeyPair ALG_EC_F2M on-card generation | | |
| ALG_EC_F2M LENGTH_EC_F2M_113 | yes | 0.703 |
| ALG_EC_F2M LENGTH_EC_F2M_131 | yes | 0.703 |
| ALG_EC_F2M LENGTH_EC_F2M_163 | yes | 0.719 |
| ALG_EC_F2M LENGTH_EC_F2M_193 | yes | 0.797 |
| javacard.security.KeyPair ALG_EC_FP on-card generation | | |
| ALG_EC_FP LENGTH_EC_FP_112 | no | |
| ALG_EC_FP LENGTH_EC_FP_128 | no | |