Tabelle1

Nokia 6131 phone
Card ATR: 3B:88:80:01:00:73:C8:40:13:00:90:00:71

Class javacardx.crypto.Cipher	supported
ALG_DES_CBC_NOPAD	Yes
ALG_DES_CBC_ISO9797_M1	Yes
ALG_DES_CBC_ISO9797_M2	Yes
ALG_DES_CBC_PKCS5	Yes
ALG_DES_ECB_NOPAD	Yes
ALG_DES_ECB_ISO9797_M1	Yes
ALG_DES_ECB_ISO9797_M2	Yes
ALG_DES_ECB_PKCS5	Yes
ALG_RSA_ISO14888	Yes
ALG_RSA_PKCS1	Yes
ALG_RSA_ISO9796	Yes
ALG_RSA_NOPAD	Yes
ALG_AES_BLOCK_128_CBC_NOPAD	No
ALG_AES_BLOCK_128_ECB_NOPAD	No
ALG_RSA_PKCS1_OAEP	No
ALG_KOREAN_SEED_ECB_NOPAD	No
ALG_KOREAN_SEED_CBC_NOPAD	No

Class javacard.security.Signature	
ALG_DES_MAC4_NOPAD	Yes
ALG_DES_MAC8_NOPAD	Yes
ALG_DES_MAC4_ISO9797_M1	Yes
ALG_DES_MAC8_ISO9797_M1	Yes
ALG_DES_MAC4_ISO9797_M2	Yes
ALG_DES_MAC8_ISO9797_M2	Yes
ALG_DES_MAC4_PKCS5	Yes
ALG_DES_MAC8_PKCS5	Yes
ALG_RSA_SHA_ISO9796	Yes
ALG_RSA_SHA_PKCS1	Yes
ALG_RSA_MD5_PKCS1	Yes
ALG_RSA_RIPEMD160_ISO9796	Yes
ALG_RSA_RIPEMD160_PKCS1	Yes
ALG_DSA_SHA	No
ALG_RSA_SHA_RFC2409	Yes
ALG_RSA_MD5_RFC2409	Yes
ALG_ECDSA_SHA	No
ALG_AES_MAC_128_NOPAD	No
ALG_DES_MAC4_ISO9797_1_M2_ALG3	Yes
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
Class javacard.security.KeyAgreement		
ALG_EC_SVDP_DH		No
ALG_EC_SVDP_DHC		No
Class javacard.security.MessageDigest		
ALG_SHA		Yes
ALG_MD5		Yes
ALG_RIPEMD160		Yes
ALG_SHA_256		No
ALG_SHA_384		No
ALG_SHA_512		No
Class javacard.security.RandomData		
ALG_PSEUDO_RANDOM		Yes
ALG_SECURE_RANDOM		Yes
Class javacard.security.Checksum		
ALG_ISO3309_CRC16		No
ALG_ISO3309_CRC32		No
Class javacard.security.KeyPair		
ALG_RSA	-	
	ALG_RSA LENGTH_RSA_512	Yes
	ALG_RSA LENGTH_RSA_736	Yes
	ALG_RSA LENGTH_RSA_768	Yes
	ALG_RSA LENGTH_RSA_896	Yes
	ALG_RSA LENGTH_RSA_1024	Yes
	ALG_RSA LENGTH_RSA_1280	Yes
	ALG_RSA LENGTH_RSA_1536	Yes
	ALG_RSA LENGTH_RSA_1984	Yes
	ALG_RSA LENGTH_RSA_2048	Yes
ALG_RSA_CRT	**-**	
	ALG_RSA_CRT LENGTH_RSA_512	Yes
	ALG_RSA_CRT LENGTH_RSA_736	Yes
	ALG_RSA_CRT LENGTH_RSA_768	Yes
	ALG_RSA_CRT LENGTH_RSA_896	Yes
	ALG_RSA_CRT LENGTH_RSA_1024	Yes
	ALG_RSA_CRT LENGTH_RSA_1280	Yes
	ALG_RSA_CRT LENGTH_RSA_1536	Yes
	ALG_RSA_CRT LENGTH_RSA_1984	Yes
	ALG_RSA_CRT LENGTH_RSA_2048	Yes
ALG_DSA	**-**	
	ALG_DSA LENGTH_DSA_512	No
	ALG_DSA LENGTH_DSA_768	No
	ALG_DSA LENGTH_DSA_1024	No

Tabelle1

ALG_EC_F2M	**-**	
	ALG_EC_F2M LENGTH_EC_F2M_113	No
	ALG_EC_F2M LENGTH_EC_F2M_131	No
	ALG_EC_F2M LENGTH_EC_F2M_163	No
	ALG_EC_F2M LENGTH_EC_F2M_193	No
ALG_EC_FP	**-**	
	ALG_EC_FP LENGTH_EC_FP_112	No
	ALG_EC_FP LENGTH_EC_FP_128	No
	ALG_EC_FP LENGTH_EC_FP_160	No
	ALG_EC_FP LENGTH_EC_FP_192	No
Class javacard.security.KeyBuilder		
DES_KEY		
	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
AES_KEY		
	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
RSA_PUBLIC_KEY		
	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
RSA_PRIVATE_KEY		
	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
RSA_CRT_PRIVATE_KEY		
	TYPE_RSA_CRT_PRIVATE LENGTH_RSA_512	Yes
	TYPE_RSA_CRT_PRIVATE LENGTH_RSA_736	Yes
	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
DSA_PRIVATE_KEY		
	TYPE_DSA_PRIVATE LENGTH_DSA_512	No
	TYPE_DSA_PRIVATE LENGTH_DSA_768	No
	TYPE_DSA_PRIVATE LENGTH_DSA_1024	No
DSA_PUBLIC_KEY		
	TYPE_DSA_PUBLIC LENGTH_DSA_512	No
	TYPE_DSA_PUBLIC LENGTH_DSA_768	No
	TYPE_DSA_PUBLIC LENGTH_DSA_1024	No
EC_F2M_PRIVATE_KEY		
	TYPE_EC_F2M_PRIVATE LENGTH_EC_F2M_113	No
	TYPE_EC_F2M_PRIVATE LENGTH_EC_F2M_131	No
	TYPE_EC_F2M_PRIVATE LENGTH_EC_F2M_163	No
	TYPE_EC_F2M_PRIVATE LENGTH_EC_F2M_193	No
EC_FP_PRIVATE_KEY		
	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
KOREAN_SEED_KEY		
	TYPE_KOREAN_SEED_TRANSIENT_RESET	No
	TYPE_KOREAN_SEED_TRANSIENT_DESELECT	No
	TYPE_KOREAN_SEED LENGTH_KOREAN_SEED_128	No
HMAC_KEY		
	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