Gemplus GCX4 72k PK (GemCombiXpresso + integrovaný Mifare1k) Card ATR: 3B:7A:94:00:00:80:65:A2:01:01:01:3D:72:D6:43		
javacardx.crypto.Cipher	available	time (sec)
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	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	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	no	
ALG_AES_MAC_128_NOPAD	yes	
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	

javacard.security.MessageDigest	available	time (sec)
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	yes	
TYPE_AES_TRANSIENT_DESELECT	yes	
TYPE_AES LENGTH_AES_128	yes	
TYPE_AES LENGTH_AES_192	yes	
TYPE_AES LENGTH_AES_256	yes	
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	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	
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	no	

	available	time (sec)
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	
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	available	time (sec)
ALG_RSA LENGTH_RSA_512	yes	4.391000
ALG_RSA LENGTH_RSA_736	no	
ALG_RSA LENGTH_RSA_768	yes	1.922000
ALG_RSA LENGTH_RSA_896	yes	9.812000
ALG_RSA LENGTH_RSA_1024	yes	5.766000
ALG_RSA LENGTH_RSA_1280	yes	21.547000
ALG_RSA LENGTH_RSA_1536	yes	34.765000
ALG_RSA LENGTH_RSA_1984	yes	55.188000
ALG_RSA LENGTH_RSA_2048	yes	44.828000
javacard.security.KeyPair ALG_RSA_CRT on-card generation		
ALG_RSA_CRT LENGTH_RSA_512	yes	1.844000
ALG_RSA_CRT LENGTH_RSA_736	no	
ALG_RSA_CRT LENGTH_RSA_768	yes	2.562000
ALG_RSA_CRT LENGTH_RSA_896	yes	8.703000
ALG_RSA_CRT LENGTH_RSA_1024	yes	10.985000
ALG_RSA_CRT LENGTH_RSA_1280	yes	7.484000
ALG_RSA_CRT LENGTH_RSA_1536	yes	7.016000
ALG_RSA_CRT LENGTH_RSA_1984	yes	41.734000
ALG_RSA_CRT LENGTH_RSA_2048	yes	66.141000
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	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	
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	
ALG_EC_FP LENGTH_EC_FP_160	no	
ALG_EC_FP LENGTH_EC_FP_192	no	