

SecurityServer 6.0.0

Algorithms and Key Sizes

SecurityServer 6.0.0 supports numerous algorithms for encryption / decryption, message authentication, message digest calculation / hashing, digital signature generation and verification, and key agreement. The following tables list all supported algorithms with their respective key sizes and other relevant parameters, and names the standards to which they comply.

Encryption / Decryption

Algorithms	Key size(s) (bit)	Standard
AES ECB / CBC / CFB8 / OFB / CTR	128 / 192 / 256	FIPS 197; SP 800-38A
AES CCM	128 / 192 / 256	FIPS 197, SP800-38C
AES GCM	128 / 192 / 256	FIPS 197, SP800-38D
Triple DES ECB / CBC / CFB8 (non-FIPS only)	128 / 192	SP 800-67, SP 800-38A
DES ECB / CBC / CFB8 (non-FIPS only)	64	FIPS 46-3, SP 800-38A
RSA	512 – 16384	PKCS#1 V1.5, PKCS#1 V2.1 EME-OAEP
ECC (ECIES)	112 – 571	SEC 1: Elliptic Curve Cryptography For a list of built-in Elliptic Curves see CS_PD_SecurityServer_Elliptic_Curves.pdf
SM4 ECB / CBC / CFB / OFB / CTR / GCM / CCM	128	https://datatracker.ietf.org/doc/draft-ribose-cfrg-sm4/

Message Authentication

Algorithms	Key size(s) (bit)	Standard
AES CMAC	128 / 192 / 256	FIPS 197, NIST SP 800-38B
AES GMAC	128 / 192 / 256	FIPS 197, NIST SP 800-38D
AES MAC CBC Mode	128 / 192 / 256	FIPS 197, ISO/IEC 9797
Triple DES MAC (non-FIPS only)	128 / 192	NIST SP 800-67, ANSI X9.9
Triple DES Retail-MAC (non-FIPS only)	128 / 192	NIST SP 800-67, ANSI X9.19
HMAC	160 / 224 / 256 / 384 / 512	FIPS 198-1, based on SHA-1 / SHA2 / SHA3
SM4 GMAC	128	https://datatracker.ietf.org/doc/draft-ribose-cfrg-sm4/

Message Digest

<i>Algorithms</i>	<i>Key size(s) (bit)</i>	<i>Standard</i>
SHA-1	160	FIPS 180-4
SHA2	224 / 256 / 384 / 512	FIPS 180-4
SHA3	224 / 256 / 384 / 512	FIPS 202
MD5 (non-FIPS only)	128	RFC 1321
MDC-2	128	
RIPEMD-160 (non-FIPS only)	160	https://homes.esat.kuleuven.be/~bosselae/ripemd160.html
SM3 (non-FIPS only)	256	https://datatracker.ietf.org/doc/draft-sca-cfrg-sm3/

Digital Signature Generation and Verification

<i>Algorithms</i>	<i>Key size(s) (bit)</i>	<i>Standard</i>
RSA	512 – 16384	FIPS 186-4
DSA (non-FIPS only)	1024 – 3072	FIPS 186-4
ECDSA	112 – 571	FIPS 186-4 For a list of built-in Elliptic Curves see CS_PD_SecurityServer_Elliptic_Curves.pdf
EdDSA (Ed25519)	255	RFC 8032 PureEdDSA w/ curve “edwards25519”
curve448	448	RFC 7748 with Errata ID 4730
edwards448	448	RFC 7748 with Errata ID 4730
SM2	256	https://datatracker.ietf.org/doc/draft-shen-sm2-ecdsa/



The size of RSA keys stored on smartcards and used for smartcard-based user authentication is limited to 2048 bit.

Key Agreement

Algorithms	Key size(s) (bit)	Standard
DH (non-FIPS only)	1024 – 3072	NIST SP 800-56A, ANSI X9.42
ECDH	112 – 571	NIST SP 800-56A, ANSI X9.42 For a list of built-in Elliptic Curves see CS_PD_SecurityServer_Elliptic_Curves.pdf
ECDH (X25519)	255	RFC 7748 w/ curve “curve25519”

Key Wrapping

Algorithms	Key size(s) (bit)	Standard
AES Key Wrap	128 / 192 / 256	NIST SP 800-38F (KW)
AES Key Wrap w/ padding	128 / 192 / 256	NIST SP 800-38F (KWP)
AES Key Wrap w/ PKCS#7 padding	128 / 192 / 256	KCS#11 (mechanism CKM_AES_KEY_WRAP_PAD), RFC5649