

SecurityServer 4.10 Algorithms and Key Sizes

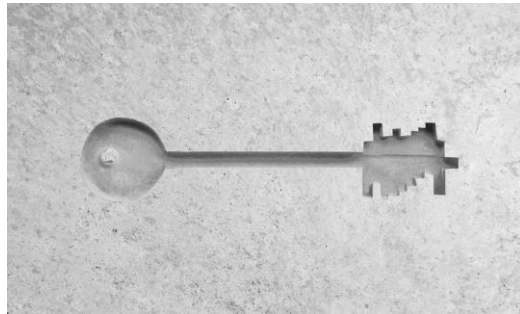
1 SecurityServer 4.10 Supported Algorithms and Key Sizes

SecurityServer 4.10 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.

Algorithms resp. Modes of Operation marked with * have been newly introduced in SecurityServer 4.10.

Encryption / Decryption

Algorithm	Key size(s) (bit)	Standard
AES ECB / CBC / CFB8 / OFB	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	128 / 192	SP 800-67, SP 800-38A
DES ECB / CBC / CFB8	64	FIPS 46-3, SP 800-38A



SecurityServer 4.10

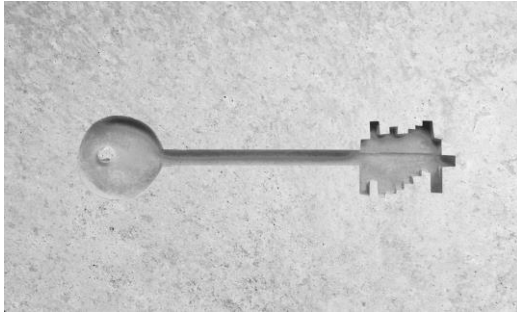
Algorithms and Key Sizes

Message Authentication

Algorithm	Key size(s) (bit)	Standard
AES CMAC	128 / 192 / 256	FIPS 197, SP 800-38B
AES GMAC *	128 / 192 / 256	FIPS 197, SP 800-38D
AES MAC CBC Mode	128 / 192 / 256	FIPS 197, ISO/IEC 9797
Triple-DES MAC	128 / 192	SP 800-67, ANSI X9.9
Triple-DES Retail-MAC	128 / 192	SP 800-67, ANSI X9.19
HMAC	160 / 224 / 256 / 384 / 512	FIPS 198-1, based on SHA-1 / SHA2 / SHA3

Message Digest

Algorithm	Hash size(s) (bit)	Standard
SHA-1	160	FIPS 180-4
SHA2	224 / 256 / 384 / 512	FIPS 180-4
SHA3 *	224 / 256 / 384 / 512	FIPS 202
MD5	128	RFC 1321
MDC-2	128	
RIPEMD-160	160	https://homes.esat.kuleuven.be/~bosselae/ripemd160.html



SecurityServer 4.10 Algorithms and Key Sizes

Digital Signature Generation and Verification

Algorithm	Key size(s) (bit)	Standard
RSA	512 – 16384	FIPS 186-4
ECDSA	112 – 571	FIPS 186-4, for a list of built-in Elliptic Curves see CS_PD_SecurityServer_4.10_Elliptic_Curves.pdf
DSA	1024 – 3072	FIPS 186-4

Key Agreement

Algorithm	Key size(s) (bit)	Standard
ECDH	112 – 571	SP 800-56A, for a list of built-in Elliptic Curves see CS_PD_SecurityServer_4.10_Elliptic_Curves.pdf