CNG Cryptographic Algorithm Providers

learn.microsoft.com/en-us/windows/win32/seccertenroll/cng-cryptographic-algorithm-providers

- Article
- 01/26/2023

In this article

1. Symmetric Algorithms
2. Asymmetric Algorithms
3. Hashing Algorithms
4. Key Exchange Algorithms
5. Related topics

Unlike Cryptography API (CryptoAPI), Cryptography API: Next Generation (CNG) separates cryptographic providers from key storage providers. Basic cryptographic algorithm operations such as hashing and signing are called primitive operations or simply primitives. CNG includes a provider that implements the following algorithms.

- Symmetric Algorithms
- Asymmetric Algorithms
- Hashing Algorithms
- Key Exchange Algorithms
- Related topics

Symmetric Algorithms

Name	Supported modes	Key size in bits (Default/Min/Max)
Advanced Encryption Standard (AES)	ECB, CBC, CFB8, CFB128, GCM, CCM, GMAC, CMAC, AES Key Wrap, XTS **Windows 8:** Support for the CFB128 and CMAC modes begins. **Windows 10:** Support for XTS-AES mode begins.	128/192/256
Data Encryption Standard (DES)	ECB, CBC, CFB8, CFB64 **Windows 8:** Support for the CFB64 mode begins.	56/56/56
Data Encryption Standard XORed(DESX)	ECB, CBC, CFB8, CFB64 **Windows 8:** Support for the CFB64 mode begins.	192/192/192

Name	Supported modes	Key size in bits (Default/Min/Max)
Triple Data Encryption Standard (3DES)	ECB, CBC, CFB8, CFB64 **Windows 8:** Support for the CFB64 mode begins.	112/168
RSA Data Security 2 (RC2)	ECB, CBC, CFB8, CFB64 modes are supported. **Windows 8:** Support for the CFB64 mode begins.	16 to 128 in 8 bit increments
RSA Data Security 4 (RC4)		8 to 512, in 8-bit increments

Asymmetric Algorithms

Name	Notes	Key size in bits (Default/Min/Max)
Digital Signature Algorithm (DSA)	Implementation conforms to FIPS 186-3 for key sizes between 1024 and 3072 bits. Implementation conforms to FIPS 186-2 for key sizes from 512 to 1024 bits.	512 to 3072, in 64-bit increments **Windows 8:** Support for the a 3072 bit key begins.
RSA	Includes RSA algorithms that use PKCS1, Optimal Asymmetric Encryption Padding (OAEP) encoding or padding, or Probabilistic Signature Scheme (PSS) plaintext padding	512 to 16384, in 64-bit increments
Elliptic Curve Digital Signature Algorithm (ECDSA)	Includes curves that use 256, 384 and 521 bit public keys as specified in FIPS 186-3. **Note:** To display all named elliptic curves, use **certutil displayEccCurve**.	256/384/521

Hashing Algorithms

Name	Notes	Key size in bits (Default/Min/Max)
Secure Hash Algorithm 1 (SHA1)	Includes HmacSha1	160/160/160
Secure Hash Algorithm 256 (SHA256)	Includes HmacSha256	256/256/256
Secure Hash Algorithm 384 (SHA384)	Includes HmacSha384	384/384/384

Name	Notes	Key size in bits (Default/Min/Max)
Secure Hash Algorithm 512 (SHA512)	Includes HmacSha512	512/512/512
Message Digest 2 (MD2)	Includes HmacMd2	128/128/128
Message Digest 4 (MD4)	Includes HmacMd4	128/128/128
Message Digest 5 (MD5)	Includes HmacMd5	128/128/128

Key Exchange Algorithms

Algorithm name	Notes	Key size in bits (Default/Min/Max)
Diffie-Hellman Key Exchange Algorithm	512 to 4096, in 64-bit increments	
Elliptic Curve Diffie-Hellman (ECDH)	Includes curves that use 256, 384 and 521 bit public keys as specified in SP800-56A.	256/384/521

Related topics

CNG Algorithm Identifiers

CNG Cryptographic Primitive Functions

Understanding Cryptographic Providers