CryptoAPI Cryptographic Service Providers

- Article
- 01/08/2021

In this article

Providers associated with Cryptography API (*CryptoAPI*) are called cryptographic service providers (CSPs) in this documentation. CSPs typically implement cryptographic algorithms and provide key storage. Providers associated with CNG, on the other hand, separate algorithm implementation from key storage. The following Microsoft CSPs are distributed with Windows Vista and Windows Server 2008.

Microsoft Base Cryptographic Provider v1.0

Implements the following algorithms to hash, sign, and encrypt content.

Name	Use	Type	Key size (Default/Min/Max)
Data Encryption Standard (DES)	Encryption	Block	56/56/56
Hashed Message Authentication Checksum (HMAC)	Hashing	Any	0/0/0
Message Authentication Checksum (MAC)	Hashing	Any	0/0/0
Message Digest 2 (MD2)	Hashing	Any	128/128/128
Message Digest 4 (MD4)	Hashing	Any	128/128/128
Message Digest 5 (MD5)	Hashing	Any	128/128/128
RSA Data Security 2 (RC2)	Encryption	Block	40/40/56
RSA Data Security 4 (RC4)	Encryption	Block	40/40/56
RSA Key Exchange	Key exchange	RSA	512/384/1024
RSA Signature	Signing	RSA	512/384/16384
Secure Hash Algorithm (SHA1)	Hashing	Any	160/160/160

Name	Use	Type	Key size (Default/Min/Max)
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hashing	Any	288/288/288

Microsoft Base DSS and Diffie-Hellman Cryptographic Provider

Implements the following algorithms to support hashing, signing, encryption, and Diffie-Hellman key exchange.

Name	Use	Type	Key size (Default/Min/Max)
CYLINK Message Encryption Algorithm	Encryption	Block	40/40/40
Data Encryption Standard (DES)	Encryption	Block	56/56/56
Diffie-Hellman Key Exchange Algorithm	Key exchange	Diffie-Hellman	512/512/1024
Diffie-Hellman Ephemeral Algorithm	Key exchange	Diffie-Hellman	512/512/1024
Digital Signature Algorithm (DSA)	Signing	DSS	1024/512/1024
Message Digest 5 (MD5)	Hashing	Any	128/128/128
RSA Data Security 2 (RC2)	Encryption	Block	40/40/56
RSA Data Security 4 (RC4)	Encryption	Stream	40/40/56
Secure Hash Algorithm (SHA1)	Hashing	Any	160/160/160

Microsoft Base DSS Cryptographic Provider

Implements the following algorithms to sign and hash content:

Name	Use	Type	Key size (Default/Min/Max)
Digital Signature Algorithm (DSA)	Signing	DSS	1024/512/1024
Message Digest 5 (MD5)	Hashing	Any	128/128/128
Secure Hash Algorithm (SHA1)	Hashing	Any	160/160/160

Microsoft Base Smart Card Crypto Provider

Supports smart cards and implements the following algorithms to hash, sign, and encrypt content.

Name	Use	Type	Key size (Default/Min/Max)
Advanced Encryption Standard 128 (AES128)	Encryption	Block	128/128/128
Advanced Encryption Standard 192 (AES192)	Encryption	Block	192/192/192
Advanced Encryption Standard 256 (AES256)	Encryption	Block	256/256/256
Data Encryption Standard (DES)	Encryption	Block	56/56/56
Two Key Triple DES	Encryption	Block	112/112/112
Three Key Triple DES	Encryption	Block	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hashing	Any	0/0/0
Message Authentication Checksum (MAC)	Hashing	Any	0/0/0
Message Digest 2 (MD2)	Hashing	Any	128/128/128
Message Digest 4 (MD4)	Hashing	Any	128/128/128
Message Digest 5 (MD5)	Hashing	Any	128/128/128
RSA Data Security 2 (RC2)	Encryption	Block	128/40/128
RSA Data Security 4 (RC4)	Encryption	Stream	128/40/128
RSA Key Exchange	Key exchange	RSA	1024/1024/4096
RSA Signature	Signing	RSA	1024/1024/4096
Secure Hash Algorithm (SHA1)	Hashing	Any	160/160/160
Secure Hash Algorithm 256 (SHA256)	Hashing	Any	256/256/256
Secure Hash Algorithm 384 (SHA384)	Hashing	Any	384/384/384
Secure Hash Algorithm 512 (SHA512)	Hashing	Any	512/512/512
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hashing	Any	288/288/288

Microsoft DH Schannel Cryptographic Provider

Supports the Secure Channel (Schannel) security package which implements Secure Sockets Layer (SSL) and Transport Layer Security (TLS) authentication protocols. This CSP also supports Diffie-Hellman key exchange and implements the following algorithms.

Name	Use	Type	Key size (Default/Min/Max)
CYLINK Message Encryption Algorithm	Encryption	Block	40/40/40
Data Encryption Standard (DES)	Encryption	Block	56/56/56
Two Key Triple DES	Encryption	Block	112/112/112
Three Key Triple DES	Encryption	Block	168/168/168
Diffie-Hellman Key Exchange Algorithm	Key exchange	Diffie-Hellman	512/512/4096
Diffie-Hellman Ephemeral Algorithm	Key exchange	Diffie-Hellman	512/512/4096
Digital Signature Algorithm (DSA)	Signing	DSS	1024/512/1024
Message Digest 5 (MD5)	Hashing	Any	128/128/128
RSA Data Security 2 (RC2)	Encryption	Block	40/40/128
RSA Data Security 4 (RC4)	Encryption	Stream	40/40/128
Secure Hash Algorithm (SHA1)	Hashing	Any	160/160/160
Schannel Encryption Key	Encryption	Schannel	0/0/-1
Schannel MAC Key	Encryption/Hashing	Schannel	0/0/-1
Schannel Master Hash	Encryption/Hashing	Schannel	0/0/-1
Secure Sockets Layer (SSL3) Master	Encryption	Schannel	384/384/384
Transport Layer Security (TLS1) Master	Encryption	Schannel	384/384/384

Microsoft Enhanced Cryptographic Provider v1.0

Provides stronger security than the Microsoft Base Cryptographic Provider v1.0 by using longer keys with some of the existing algorithms and by implementing additional algorithms.

Name	Use	Type	Key size (Default/Min/Max)
Data Encryption Standard (DES)	Encryption	Block	56/56/56
Two Key Triple DES	Encryption	Block	112/112/112
	Encryption	Block	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hashing	Any	0/0/0
Message Authentication Checksum (MAC)	Hashing	Any	0/0/0
Message Digest 2 (MD2)	Hashing	Any	128/128/128
Message Digest 4 (MD4)	Hashing	Any	128/128/128
Message Digest 5 (MD5)	Hashing	Any	128/128/128
RSA Data Security 2 (RC2)	Encryption	Block	128/40/128
RSA Data Security 4 (RC4)	Encryption	Stream	128/40/128
RSA Key Exchange	Key exchange	RSA	1024/384/16384
RSA Signature	Signing	RSA	1024/384/16384
Secure Hash Algorithm (SHA1	Hashing	Any	160/160/160
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hashing	Any	288/288/288

Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider

Provides stronger security than the Microsoft Base DSS and Diffie-Hellman Cryptographic Provider CSP by using longer keys with some of the existing algorithms and by implementing additional algorithms.

Name	Use	Type	Key size (Default/Min/Max)
CYLINK Message Encryption Algorithm	Encryption	Block	40/40/40
Data Encryption Standard (DES)	Encryption	Block	56/56/56
Two Key Triple DES	Encryption	Block	112/112/112
Three Key Triple DES	Encryption	Block	168/168/168

Name	Use	Type	Key size (Default/Min/Max)
Diffie-Hellman Key Exchange Algorithm	Key exchange	Diffie-Hellman	1024/512/4096
Diffie-Hellman Ephemeral Algorithm	Key exchange	Diffie-Hellman	1024/512/4096
Digital Signature Algorithm (DSA)	Signing	DSS	1024/512/1024
Message Digest 5 (MD5)	Hashing	Any	128/128/128
RSA Data Security 2 (RC2)	Encryption	Block	128/128/128
RSA Data Security 4 (RC4)	Encryption	Stream	128/128/128
Secure Hash Algorithm (SHA1)	Hashing	Any	160/160/160

Microsoft Enhanced RSA and AES Cryptographic Provider

Implements the following algorithms to sign, encrypt, and hash content.

Name	Use	Type	Key size (Default/Min/Max)
Advanced Encryption Standard 128 (AES128)	Encryption	Block	128/128/128
Advanced Encryption Standard 192 (AES192)	Encryption	Block	192/192/192
Advanced Encryption Standard 256 (AES256)	Encryption	Block	256/256/256
Data Encryption Standard (DES)	Encryption	Block	56/56/56
Two Key Triple DES	Encryption	Block	112/112/112
Three Key Triple DES	Encryption	Block	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hashing	Any	0/0/0
Message Authentication Checksum (MAC)	Hashing	Any	0/0/0
Message Digest 2 (MD2)	Hashing	Any	128/128/128
Message Digest 4 (MD4)	Hashing	Any	128/128/128
Message Digest 5 (MD5)	Hashing	Any	128/128/128
RSA Data Security 2 (RC2)	Encryption	Block	128/128/128

Name	Use	Type	Key size (Default/Min/Max)
RSA Data Security 4 (RC4)	Encryption	Stream	128/128/128
RSA Key Exchange	Key exchange	RSA	1024/384/16384
RSA Signature	Signing	RSA	1024/384/16384
Secure Hash Algorithm (SHA1)	Hashing	Any	160/160/160
Secure Hash Algorithm (SHA256)	Hashing	Any	256/256/256
Secure Hash Algorithm (SHA384)	Hashing	Any	384/384/384
Secure Hash Algorithm (SHA512)	Hashing	Any	512/512/512
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hashing	Any	288/288/288

Microsoft RSA Schannel Cryptographic Provider

Supports the RSA Secure Channel (Schannel) security package which implements Secure Sockets Layer (SSL) and Transport Layer Security (TLS) authentication protocols.

Name	Use	Type	Key size (Default/Min/Max)
Advanced Encryption Standard 128 (AES128)	Encryption	Block	128/128/128
Advanced Encryption Standard 256 (AES256)	Encryption	Block	256/256/256
Data Encryption Standard (DES)	Encryption	Block	56/56/56
Two Key Triple DES	Encryption	Block	112/112/112
Three Key Triple DES	Encryption	Block	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hashing	Any	0/0/0
Message Authentication Checksum (MAC)	Hashing	Any	0/0/0
Message Digest 5 (MD5)	Hashing	Any	128/128/128
RSA Data Security 2 (RC2)	Encryption	Block	128/128/128
RSA Data Security 4 (RC4)	Encryption	Stream	128/128/128
RSA Key Exchange	Key exchange	RSA	1024/384/16384

Name	Use	Type	Key size (Default/Min/Max)
Schannel Encryption Key	Encryption	Schannel	0/0/-1
Schannel Master Hash	Encryption/Hashing	Schannel	0/0/-1
Schannel MAC Key	Encryption/Hashing	Schannel	0/0/-1
Secure Hash Algorithm (SHA1)	Hashing	Any	160/160/160
Secure Socket Layer 2 (SSL2) Master	Encryption	Schannel	40/40/192
Secure Socket Layer 3 (SSL3) Master	Encryption	Schannel	384/384/384
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hashing	Any	288/288/288
Transport Layer Security (TLS1) Master	Encryption	Schannel	384/384/384

Microsoft Strong Cryptographic Provider

Implements the following algorithms.

Name	Use	Type	Key size (Default/Min/Max)
Data Encryption Standard (DES)	Encryption	Block	56/56/56
Two Key Triple DES	Encryption	Block	112/112/112
Three Key Triple DES	Encryption	Block	168/168/168
Hashed Message Authentication Checksum (HMAC)	Hashing	Any	0/0/0
Message Authentication Checksum (MAC)	Hashing	Any	0/0/0
Message Digest 2 (MD2)	Hashing	Any	128/128/128
Message Digest 4 (MD4)	Hashing	Any	128/128/128
Message Digest 5 (MD5)	Hashing	Any	128/128/128
RSA Data Security 2 (RC2)	Encryption	Block	128/40/128
RSA Data Security 4 (RC4)	Encryption	Stream	128/40/128
RSA Key Exchange	Key exchange	RSA	1024/384/16384

Name	Use	Type	Key size (Default/Min/Max)
RSA Signature	Signing	RSA	1024/384/16384
Secure Hash Algorithm (SHA1)	Hashing	Any	160/160/160
Secure Socket Layer 3 SHA and MD5 (SSL3 SHAMD5)	Hashing	Any	288/288/288

Related topics

Understanding Cryptographic Providers