

# RSA/Schannel Provider Algorithms

 [learn.microsoft.com/en-us/windows/win32/seccrypto/rsa-schannel-provider-algorithms](https://learn.microsoft.com/en-us/windows/win32/seccrypto/rsa-schannel-provider-algorithms)

- Article
- 01/08/2021

The following algorithms might be supported by the Microsoft *RSA/Schannel* Cryptographic Provider.

Algorithm ID	Description	Comments
CALG_RSA_KEYX	RSA public key <u>key exchange algorithm</u>	Key length: Can be set, 384 bits to 16,384 bits in 8 bit increments. Default key length: 1,024 bits.
CALG_MD5	MD5 hashing algorithm.	Provided only for hashing.
CALG_SHA	SHA hashing algorithm.	Must be used for DSS signatures.
CALG_RC2	RC2 block encryption algorithm.	Key length: 40 to 88 bits
CALG_RC4	RC4 stream encryption algorithm.	Key length: 40 to 88 bits