Microsoft RSA/Schannel Cryptographic Provider

- Article
- 07/09/2021

The Microsoft *RSA*/*Schannel* Cryptographic Provider supports hashing, data signing, and signature verification. The algorithm identifier CALG_SSL3_SHAMD5 is used for SSL 3.0 and TLS 1.0 client authentication. This CSP supports key derivation for the SSL2, PCT1, SSL3, and TLS1 protocols. The *hash* consists of a concatenation of a MD5 hash with a SHA hash and signed with a RSA *private key*. It can be exported to other countries/regions.

	Value
Provider type	PROV_RSA_SCHANNEL
Provider name	MS_DEF_RSA_SCHANNEL_PROV

For more information about RSA/Schannel providers, see CSP Functions.