

Microsoft DSS and Diffie-Hellman/Schannel Cryptographic Provider

 learn.microsoft.com/en-us/windows/win32/seccrypto/microsoft-dss-and-diffie-hellman-schannel-cryptographic-provider

- Article
- 07/09/2021

The Microsoft DSS and Diffie-Hellman/Schannel Cryptographic Provider supports hashing, data signing with DSS, generating Diffie-Hellman (D-H) keys, exchanging D-H keys, and exporting a D-H key. This CSP supports key derivation for the SSL3 and TLS1 protocols. It can be exported to other countries/regions.

Value	
Provider type	PROV_DH_SCHANNEL
Provider name	MS_DEF_DH_SCHANNEL_PROV