

Version	2	3.0	3.1	3.2
Hash	MD5, SHA-1	SHA-1	SHA-1	SHA-256
Signature	RSA	DSA	DSA, RSA	RSA with SHA-256
Public-Key Encryption	RSA	Diffie-Hellman [52]	RSA	RSA
Symmetric Encryption	RC2/40, TripleDES CBC	TripleDES CBC	TripleDES CBC	AES-128 CBC