Legend for Notes/Description Field for NIST SP 800-135

Last Update: 04.13.2012

The following notation is used to describe the implemented features that were successfully tested.

IKE v1	AUTH ([DSA], [PKE], [[PSK])	Authentication method determines the inputs and method for computing SKEYID. DSA – digital signatures used for authentication PKE – public key encryption used for authentication PSK – pre-shared key used for authentication
	GROUP([2], [4], [14])	Well-known groups: Group 2 (1024 bit MODP), Group 4 (185 bit EC2N), Group 14 (2048 bit MODP) Used to determine size of Diffie-Hellman shared secret
	SHA([1], [224], [256], [384], [512])	HMAC SHA functions supported
	Example: AUTH(DSA, PKE, PSK) GROUP(2,14) SHA(1, 256)	
IKE v2	GROUP([2], [4], [14])	Well-known groups Group 2 (1024 bit MODP), Group 4 (185 bit EC2N), Group 14 (2048 bit MODP) Used to determine size of Diffie-Hellman shared secret
	SHA([1], [224], [256], [384], [512])	HMAC SHA functions supported
	Example: GROUP(2, 4) SHA(1, 256)	
TLS	TLS 1.0/1.1	TLS KDF used in TLS versions 1.0 and 1.1
	TLS 1.2 ([SHA-256], [SHA-384], [SHA-512])	TLS KDF used in TLS 1.2 with HMAC SHA function

		supported
	Example: TLS 1.0/1.1, TLS 1.2 (SHA-256, SHA-384)	
ANS X9.63-2001	SHA([1], [224], [256], [384], [512])	SHA functions supported
	Example: SHA(1, 224, 256)	
SSH	SHA([1], [224], [256], [384], [512])	SHA functions supported
	Example: SHA(1, 224, 256, 512)	
SRTP	AES([128], [192], [256])	AES function (key length) supported
	Example: AES(128, 256)	
SNMP	*None*	
TPM	*None*	