Legend for Description Field for Historical List for All of SP800-56A EXCEPT KDF

Last Update: 1/1/2014

NOTICE: The SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths goes into effect January 1, 2014. Key lengths (modulus and curve sizes) providing less than 112 bits of security strength are no longer approved to generate digital signatures. Therefore, the modulus size 1024 (FA Parameter Set) and the curve sizes P-192, K-163 and B-163 (EA Parameter Set) have been removed. The SP800-131A document also disallows the use of SHA-1 with Digital Signature Generation beginning January 1, 2014. All of the disallowed features of the Components validation have been moved to this Historical Components Validation List for reference.

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

ALG([FFC] [ECC])	Finite Field Cryptography, Elliptic Curve Cryptography
For FFC, SCHEMES([HYBRID1] [MQV2] [EPHEM] [HYBRID1FLOW] [MQV1] [ONEFLOW] [STATIC]) For ECC, SCHEMES ([FULLUNIF] [FULLMQV] [EPHEMUNIF] [ONEPASSUNIF] [ONEPASSMQV] [ONEPASSDH] [STATICUNIF])	Key Agreement Schemes. Refer to SP800-56A for details on the specific schemes.
KAROLES([INITIATOR] [RESPONDER]	Key Agreement Roles
For FFC, PARAMSET([FA]) For ECC, PARAMSET([EA]))	Parameter Sets supported by IUT. Refer to Section 5.5.1.1 Table 1 for the FFC Parameter Size Sets and Section 5.5.1.2 Table 2 for the ECC Parameter Size Sets.

For FFC,
PARAMSET([FA])
For ECC,
PARAMSET([EA])
	The NIST-recommended ECDSA curves supported by the IUT.

Functions included in implementation	These are functions included in the implementation of SP800-56A. They may be described in supporting documents or in the SP800-56A document. If the function is described in a supporting document,

	that function will be tested as a prerequisite for this implementation. They are used by the validation testing to test the implementation thoroughly. They include: 1. Domain Parameter Generation (DPG) (Described in 186-3 DSA – PQGGen) 2. Domain Parameter Validation (DPV) (Described in 186-3 DSA – PQGVer) 3. Key Pair Generation (KPG)) (Described in 186-3 DSA – KeyPairGen and 186-3 ECDSA – Key Pair) 4. Full Validation (Section 5.6.2.4 and/or 5.6.2.5)(Described in 186-3 ECDSA – PKV and Key Pair Generation) 5. Partial Validation (Section 5.6.2.6 (ECC only)) 6. Key Regeneration(Described in 186-3 ECDSA – PKV and Key Pair Generation)

The DLC Primitive validation process requires the following prerequisite testing:
1. The underlying DSA and/or ECDSA algorithm's functions determined by the "Functions included in the implementation". See above.