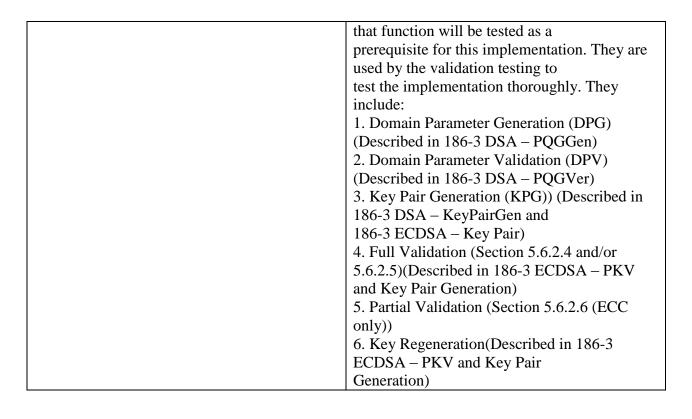
Legend for Description Field for Historical List for All of SP800-56A EXCEPT KDF

Last Update: 1/1/2014

NOTICE: The <u>SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths</u> 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,	Key Agreement Schemes. Refer to SP800-56A
SCHEMES([HYBRID1]	for details on the specific
[MQV2] [EPHEM]	schemes.
[HYBRID1FLOW] [MQV1]	
[ONEFLOW] [STATIC])	
For ECC,	
SCHEMES ([FULLUNIF]	
[FULLMQV] [EPHEMUNIF]	
[ONEPASSUNIF]	
[ONEPASSMQV]	
[ONEPASSDH]	
[STATICUNIF])	
KAROLES([INITIATOR]	Key Agreement Roles
[RESPONDER]	
For FFC,	Parameter Sets supported by IUT. Refer to
PARAMSET([FA])	Section 5.5.1.1 Table 1 for the FFC
For ECC,	Parameter Size Sets and Section 5.5.1.2 Table
PARAMSET([EA])	2 for the ECC Parameter Size
)	Sets.
For FFC,	The NIST-recommended ECDSA curves
PARAMSET([FA])	supported by the IUT.
For ECC,	
PARAMSET([EA])	
Functions included in	These are functions included in the
implementation	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,



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.