

## Legend for Description Field for Historical FIPS 186-3 ECDSA Signature Generation Component

*Last Update: 01.01.2014*

***NOTICE: The [SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths](#) goes into effect January 1, 2014. Key lengths (curve sizes) providing less than 112 bits of security strength are no longer approved to generate digital signatures. Therefore, the curve sizes P-192, K-163 and B-163 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.

<b>( CURVES ( P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1) P-256: (SHA-1) P-384: (SHA-1) P-521: (SHA-1) K-163: (SHA-1, 224,256, 384, 512) K-233: (SHA-1) K-283: (SHA-1) K-409: (SHA-1) K-571: (SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233: (SHA-1) B-283: (SHA-1) B-409: (SHA-1) B-571: (SHA-1)))</b>	List of Curves/SHA combinations tested
---	--

DRBG or RNG is a prerequisite to Signature Generation Component testing (because of the per message secret number).