Legend for Description Field for the Historical SP800-56A Section 5.7.1.2 Elliptic Curve Cryptography Cofactor Diffie-Hellman (ECCCDH) Primitive

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. 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.

Curve Tested([P-192][K-163][B-163]	Curves tested using the ECC CDH Primitive

There are no prerequisites for ECC CDH Primitive Component testing.