

**Legend for Description Field for RSADP Basic Decryption Component**  
***Last Update: 04.11.16***

***NOTICE: The SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths goes into effect January 1, 2014. The SP800-131A document disallows 80 bits of security.***

This component test tests the RSADP function as described in SP800-56B Section 7.1.2. RSADP is the basic decryption operation. It recovers keying material from ciphertext using an RSA private key. Modulus size 2048 is the only modulus size allowed in RSADP.

The following notation is used to indicate the test was successfully tested:

**RSADP:** (Mod2048)

There are no prerequisites for RSADP Component testing.