Legend for Description Field for Historical RSASP1 Signature Primitive 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. The SP800-131A document disallows the use of SHA-1 with Digital Signature Generation beginning January 1, 2014. Therefore SHA 1 has been removed from the working Component Validation List and recorded in this Historical Component Validation List.

This component test tests the RSASP1 function as described in PKCS#1 v2.1:RSA Cryptography Standard, June 14, 2002, Section 5.2.1. It applies to both the PKCS1.5 and PKCS PSS algorithms.

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

Tested(ALG[RSASSAPKCS1_V1_5] (2048 SHA(1)))	Algorithm tested: RSASSA-PKCS1_v1_5; RSASSA-PSS For RSASSA-PKCS1_v1_5: Mod/SHA combinations tested. Note: Mod/SHA size does not affect RSASSAPSS function – Function is same for all Mod/SHA sizes. Therefore, this information is not recorded.

There are no prerequisites for RSASP1 Component testing.