Legend for Description Field for RSASP1 Signature Primitive Component

***Last Update:* 03.18.2014**

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 this legend.

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.

In March 2014, the validation testing for RSASP1 was modified to include only the RSASP1 function. Prior to this, the test was also looking at the format of the input data. The RSASP1 function doesn't evaluate the format of the input data. It just expects an input string. The intended use of this function is outside the scope of the RSASP1 function. Therefore, references to the PKCS1.5 or PKCS PSS algorithms have been removed for future validations.

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

Tested(Mod 2048)	Mod size tested for RSASP1 function	For validations after March 18, 2014
Tested(ALG[RSASSAPKCS1_V1_5] (2048SHA(224,256)), ALG[RSASSA-PSS])	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.	For validation before March 18, 2014

There are no prerequisites for RSASP1 Component testing.